Certified Data Centre Design (CDCD®) – Core Unit

Introduction

Version 1509

CDCDP

Moodle Login Process

- Open Internet Explorer (v.11) browser
- Enter http://online-cnet-training.com
- Go to Login tab (top left)
- Username: Allocated by CNet Training (first name and surname, lower case - no spaces)
- Password: CNetTraining99
- Select 'My Courses' (right side), then designated course
- Select module and press enter
- Work through the module content with Instructor (use forward arrow not start arrow)
- On completion, 'Exit Activity' (right side)
- Scroll down and select the next module

© CNet Training

About CNet Training

- Designing and delivering training since 1996
- The only professional training provider in the world to award both industry-recognised qualifications and certifications
- Train in locations throughout the world
- Design and develop programs with our own experienced experts, and by working with the industry itself
- Multi award-winning
- Each CNet Training program awards both an industry-recognised qualification (awarded by Pearson Edexcel) and an official certification

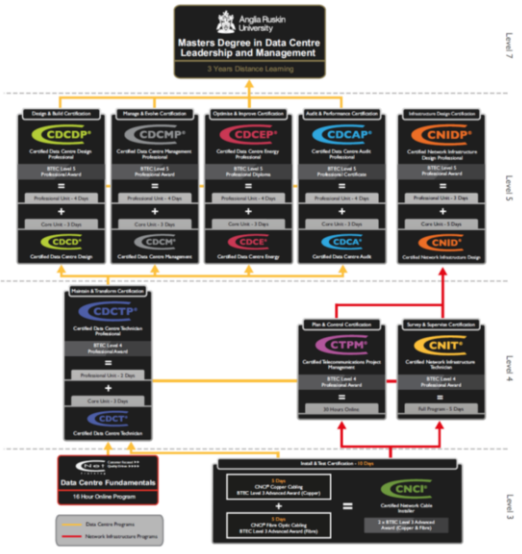
© CNet Training

About CNet Training

- Qualifications are awarded for life and confirm knowledge of a subject at a particular time
- Certifications are a commitment to lifelong learning. They require recertifying every three years and therefore provide the perfect portal to keep knowledge up-to-date with technological advancements
- CNet are the originators of The Global Data Centre and Network Infrastructure Education Framework – mapping professional learning and education from entry level through master's degree

© CNet Training

The Global Data Centre & Network Infrastructure Education Framework



- Maps professional programs to actual roles within the industry
- Provides a trusted and proven route to furthering knowledge, qualification and certification
- Programs from entry level through master's degree

© CNet Training

Joint Commitment to Learning

We will:

- Provide a conducive training environment
- Provide appropriate training material
- Provide real life experience and supporting material
- Provide the opportunity for you to network with your peers
- Answer your questions
- Enjoy the experience

You will:

- Respect your environment
- Adhere to course timings
- Switch off mobile phones
- Refrain from using laptops unless instructed
- Take advantage of the opportunity
- Participate constructively in group activities
- Enjoy the experience

© CNet Training

Course Overview

- The purpose of this course is to ensure the student will:
  - Appreciate the purpose of a Data Centre
  - Operate as part of a multi-disciplinary team
  - Establish a common vocabulary to hold a meaningful discussion with all parties in the team
  - Demonstrate an understanding of the key technology areas
  - Use current thinking and relevant standards to enable a flexible approach to design
  - Demonstrate sufficient knowledge to pass the Certified Data Centre Design (CDCD®) qualification

© CNet Training

Modular Approach

- The course consists of a number of topics which are dealt with in a series of modules
- The modules are intended to support interactive discussions
- Given topics may be familiar to some students, but hopefully you will all learn something new

© CNet Training

Course Assessment

- You will be assessed at the end of the course
- The assessment consists of 40 multiple-choice questions
- You have 75 minutes to complete the assessment
- The assessment is 'open book'
- There will also be design case study exercises undertaken throughout the course, which will be a major contributor to the overall assessment
- Course participation will also contribute to the final result

© CNet Training

Class Introductions

- Who you are?
- Who do you work for?
- What is your role in the Data Centre?
- How long have you been in this role?
- What is the biggest challenge you face in the Data Centre today?
- What is the main 'takeaway' you want from this course?

© CNet Training

Course Programme

- What is a Data Centre?
- Design planning process
- Scoping the requirement
- Raised access floor
- Cabinets
- Power
- Cooling
- Earthing and bonding
- Cable containment
- Delivering the IT strategy
- Copper and optical fibre cable connectivity
- Safety and management
- Commissioning and handover

CDCDP

© CNet Training

Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

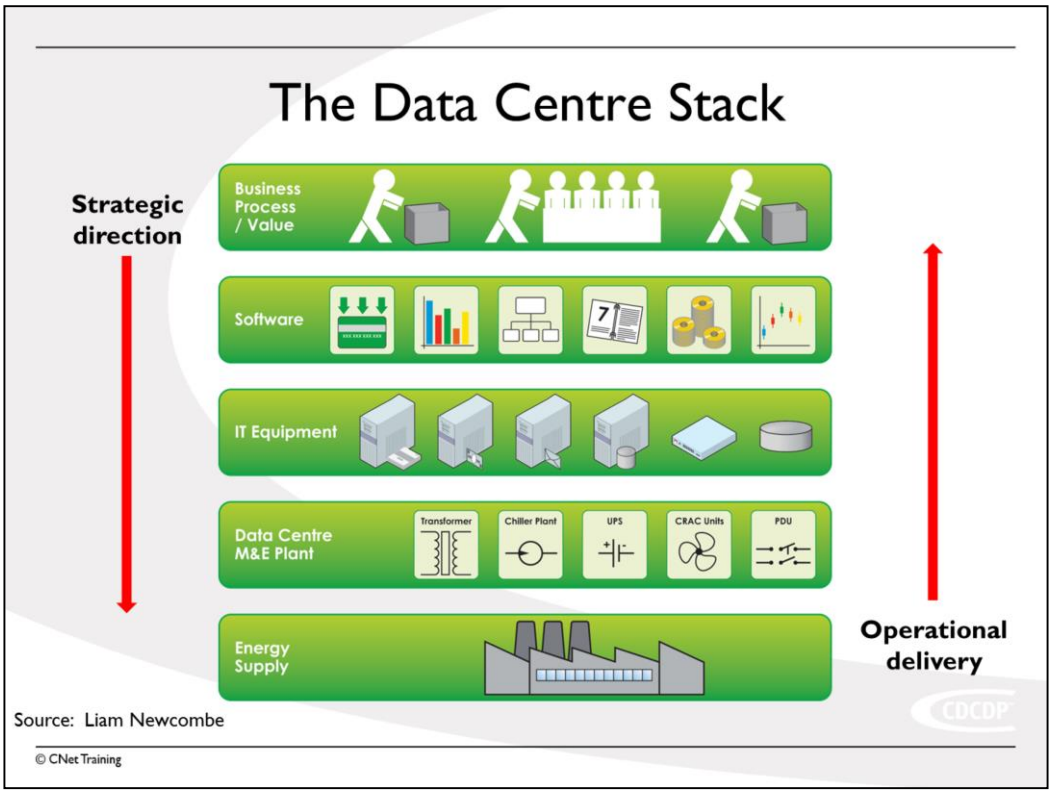
What is a Data Centre?

Version 1509

Objectives

- At the end of this module you will be able to:
  - Identify the business need
  - Define a Data Centre
  - Identify the main Data Centre types

© CNet Training



The Data Centre only exists to support the IT strategy, which in turn supports the Business needs.

We start off by sourcing energy from a supply. This energy is then delivered through the mechanical and engineering (M&E) plant to the IT equipment, which runs the application software that supports the business activities that the Data Centre is there for.

What is a Data Centre?

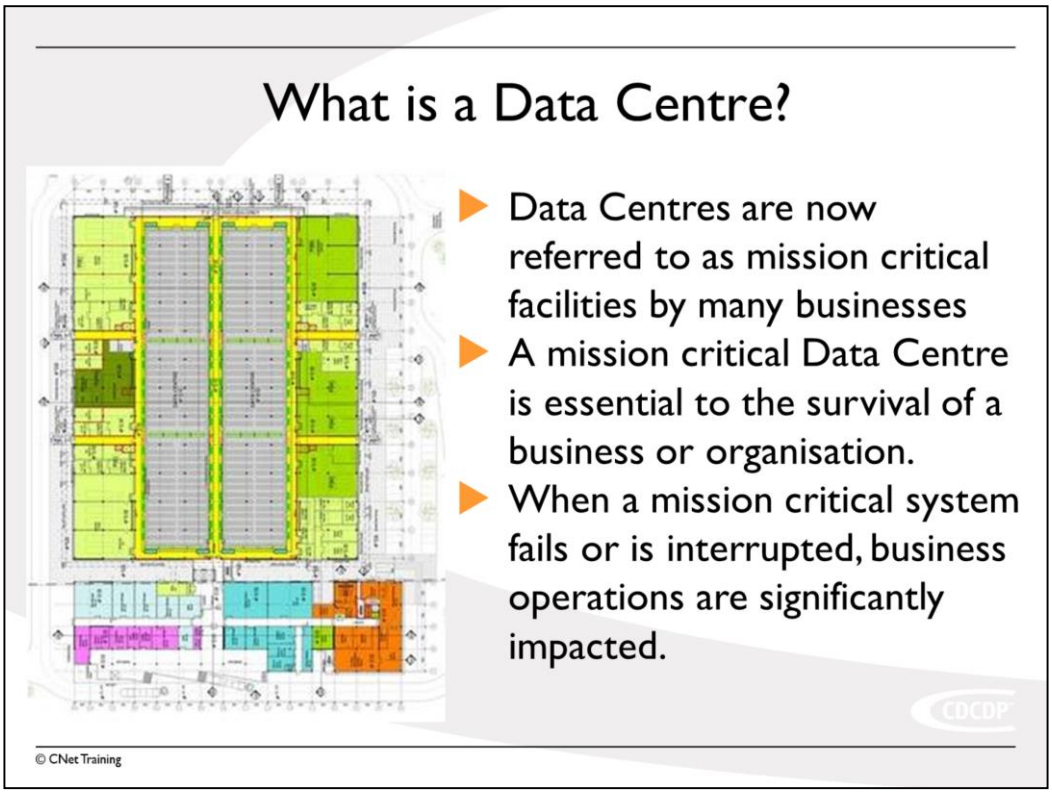
- "A building, or portion of a building, whose primary function is to house a computer room and its support areas." **Source: TIA 942-A**
- "All buildings, facilities and rooms which contain enterprise servers, server communication equipment, cooling equipment and power equipment, and provide some form of data service" **Source: EU Code of Conduct**
- "A Data Centre is a centralised repository, either physical or virtual, for the storage, management, and dissemination of data and information organised around a particular body of knowledge or pertaining to a particular business" **Source: TechTarget**

© CNet Training

The term Data Centre is used by many people to mean many things.

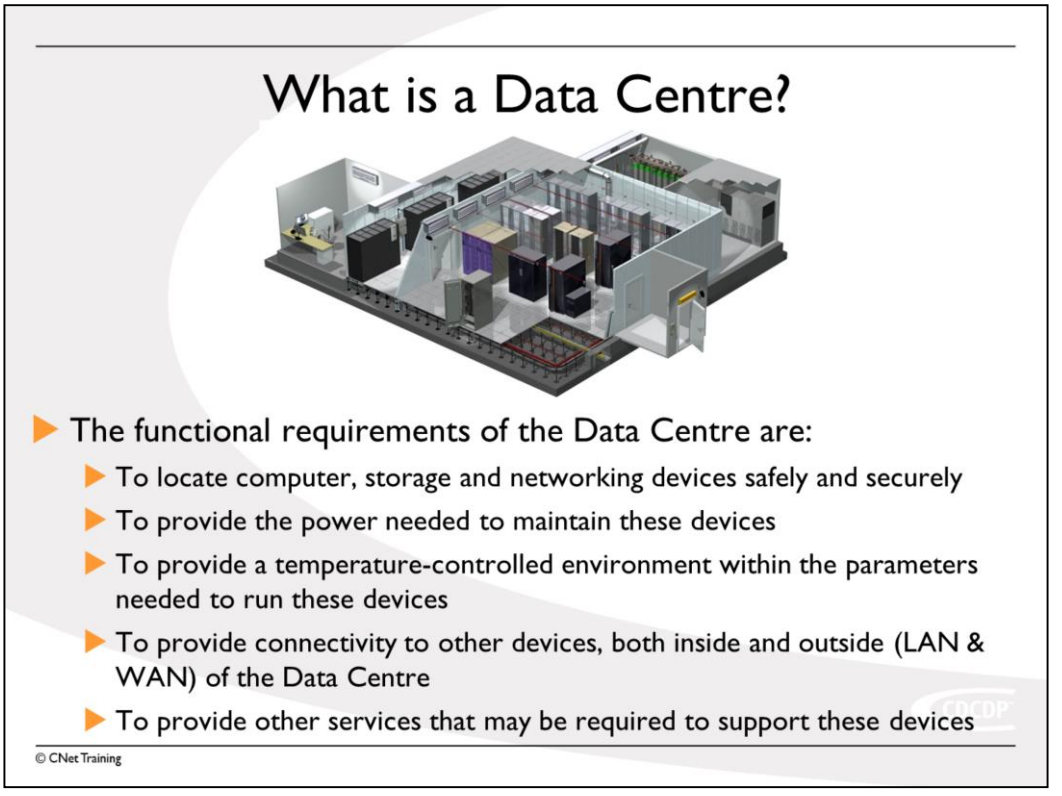
- There is no fixed size or complexity for a Data Centre, it can range from a single room up to a large complex with several computer rooms each one containing many racks of equipment.
- TIA 942-A sets out the aspects which are applicable to a Data Centre space for its availability.
- TIA 942-A defines it as shown above, but it is still open to interpretation.
- TIA 942-A sets out good principles for Data Centres. However, it is not definitive for every instance and there are often variations that can be made.
- TIA 942-A can be used as the basis for a Data Centre telecommunications design, providing the minimum infrastructure requirement's that should be expected.

The key thing is that it is "fit for purpose".



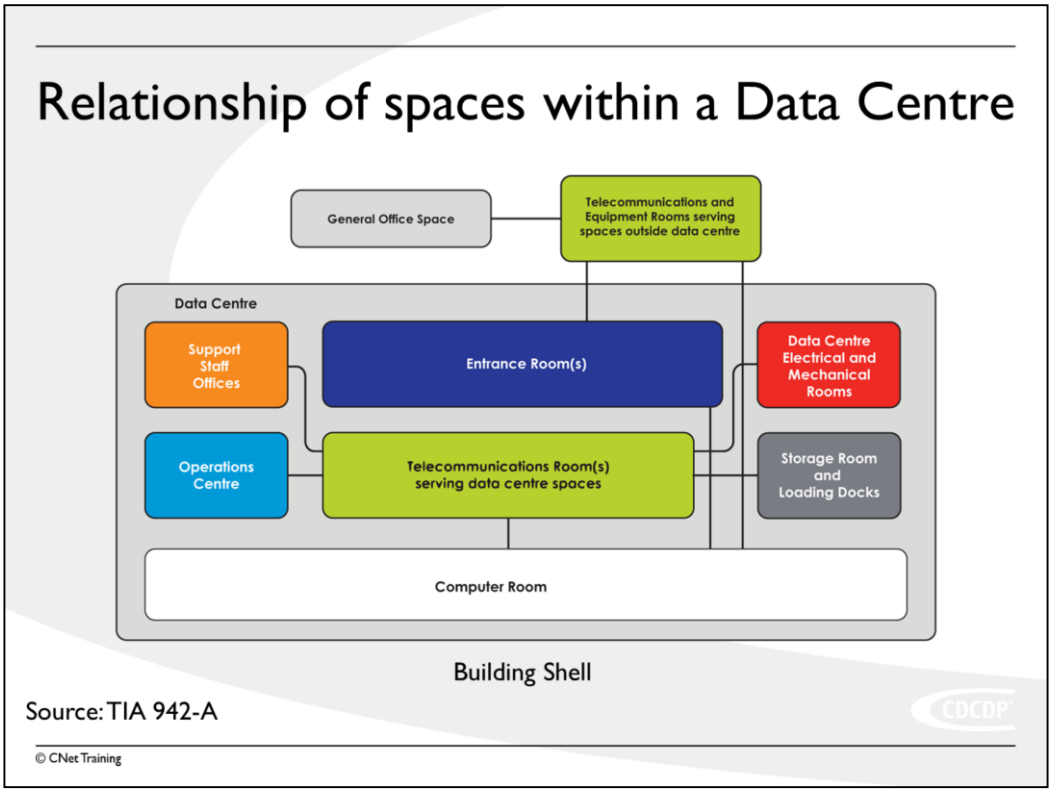
Data Centres are the mainstay of mission critical facilities, and in recent years, there has been a great deal of attention given to the Total Cost of Ownership (TCO) where the Capital Expenditure (CAPEX) and Operational Expenditure (OPEX) are scrutinised to optimise the TCO. This approach has been emphasised strongly during the recent economic downturn, and there is increasing demand on the engineering design aspect of the mission critical facility to reduce both CAPEX and OPEX by employing integrated design principles that lead to a more efficient and sustainable mission critical facility.

(Source: Consulting – Specifying Engineer)



It can be more useful to think in terms of function, because all modern Data Centres have similar requirements, both structurally and in the provisioning of services.

In order to successfully provide the planned services, it is important that continual functioning of the Data Centre infrastructure is achieved. This is the CDCD's primary consideration.



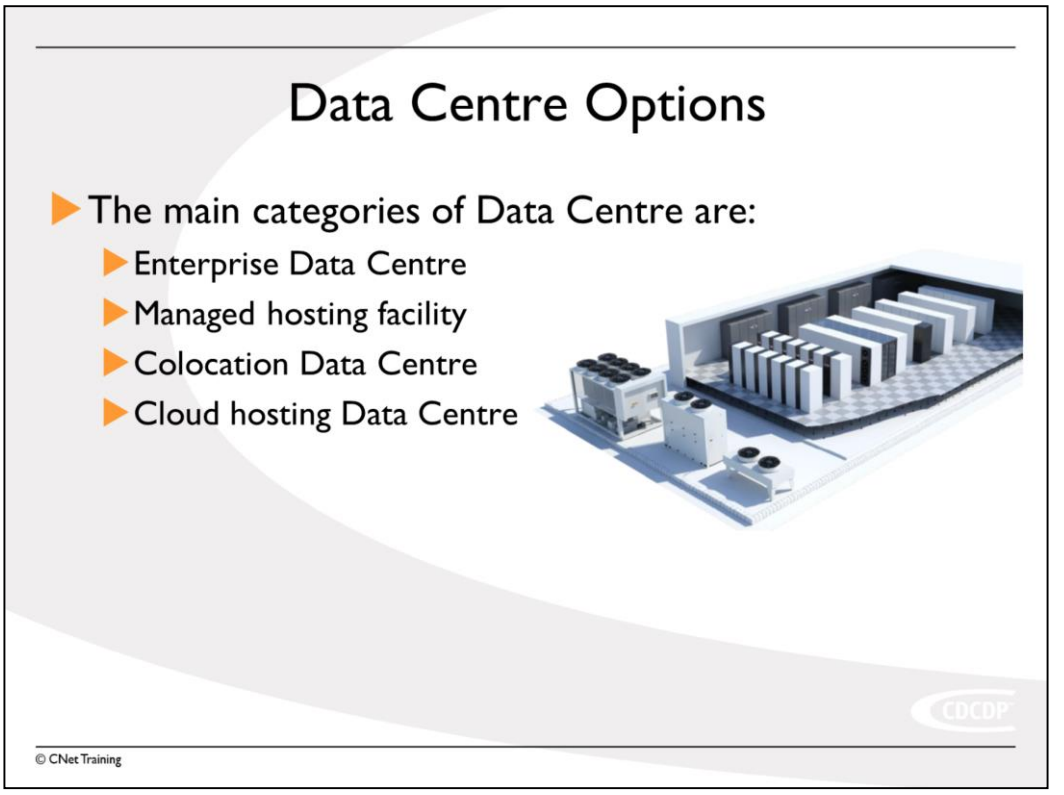
During the design phase of the Data Centre, it is important to determine the relationship of space required for the supporting facilities, as well as for the computer room.

Space allocation must be addressed as early as possible when discussing needs with the other parties (e.g. architect, structural engineer, etc.). The space may have some restrictions and subsequently result in a smaller Data Centre.

Business Considerations

- Selecting a Data Centre is a major business decision with many factors to consider:
  - Reason for design initiation
  - Desired Data Centre services
  - Business benefit
  - Financial requirement
  - Resource requirement
  - Timescale

© CNet Training



Data Centre design involves high levels of engineering for a technologically complex computer facility. It is therefore important to understand that the design process differs significantly in its approach when compared to more traditional commercial premises.

Any organisation that tries to design a Data Centre in the same way as they would design an office is doomed to fail.

The four main categories of Data Centres are shown above. The size and complexity may vary significantly depending on the type of Data Centre, but the principles applied are essentially the same.

Enterprise Data Centre

- An enterprise Data Centre is owned and operated by the same company and is sometimes located within the same facility as the main company premises, but may be located on separate site
- Can be extremely good, but ….
- Can be not so good, and fail to reach maximum potential
  - Fear of handing over
  - Egoism and empires

© CNet Training

Enterprise Data Centres tend to house all, or the majority of a company's data processing resources.

Many organisations, particularly larger ones, have chosen to provide and operate their own Data Centre. This is for a number of reasons, including:

- Security and control of the data, commercial sensitivities, etc.
- Reliability and availability of services
- Ability to respond to changing requirements
- Response time to a call for the data
- Better integration of corporate processes

Some organisations fail to gain the full potential of the Data Centre because their culture prevents them from doing so.

Managed Hosting Facility

- A hosted Data Centre is a facility managed on behalf of a business, usually located within a separate premises to the main business it is supporting
- Often referred to as outsourcing

© CNet Training

Managed hosting facilities are becoming more attractive to some businesses because they can rent IT infrastructure instead of investing in it themselves. Servers, networks, applications, bandwidth and other equipment are managed by employees of the facility.

Some businesses, initially small to medium enterprises (SMEs), view the need for data storage, servers and high capacity network connectivity as not something they either want to, or are able to, manage themselves.

Businesses that need constant network connectivity and redundant power may not have the capital to invest in the infrastructure. Many SMEs do not want to invest in Data Centre infrastructure and staffing but they still need a reliable network for internal applications and email.

An SME can rent a few servers on a monthly basis and can add servers and storage continually as it grows. It can also increase temporarily during busy periods of the year. SMEs say they like this approach as they can concentrate on their core business.

There are also reported cost advantages for SMEs with dramatic savings, compared to owning, managing and operating their own facility.

Colocation Data Centre

- A Colocation (Colo) facility is generally a larger Data Centre, which is subdivided to support many different business users
- There are different levels of service:
  - Colo hosts, customer provides all equipment and connectivity
  - Colo provides connectivity, customer owns servers
  - Colo owns the servers, customer provides the application
  - Customer just buys a service
- A Colo will usually benefit from economies of scale, provided it can fill the space

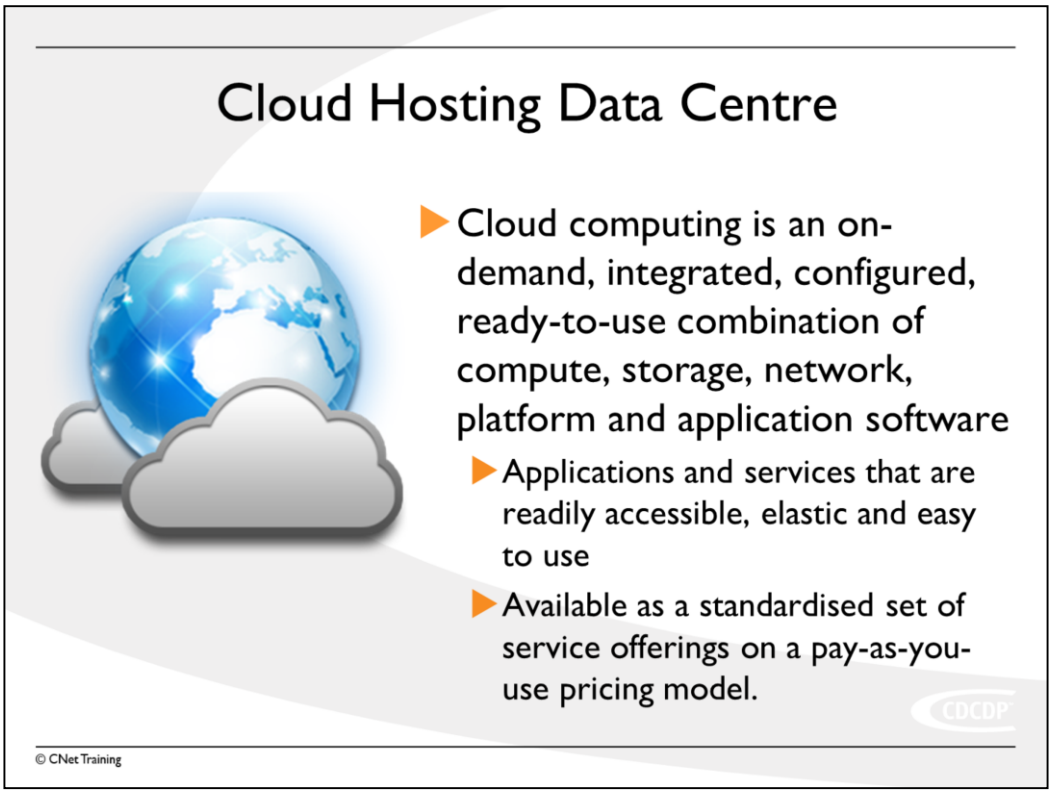
© CNet Training

The Co-location operator provides the environment for IT and telecommunications equipment housing. Service levels vary but typically the customer can have customisable units with separate shipping and receiving areas, separate entrance doors, branded lobbies and personnel. Customers can often choose their own space size, infrastructure and operational options:

- Raised floors
- Chilled water or air-side cooling
- Container-based or rack-based computer area
- Power density
- Energy efficiency

The type of customers that use co-lo facilities have evolved in recent years. A growing number of large enterprises and even some financial institutions run their Data Centres at Co-location facilities. Claimed benefits of Co-location include:

- A predictable and operational expenditure model
- Additional capacity can be brought on quickly, cheaply, and only as needed
- Better access to space and power
- Experienced professionals managing your Data Centre facility
- An ecosystem of partners in the same facility
- Dedicated infrastructure to build your cloud strategy
- Lean infrastructure to manage during times of rapid business change
- A better road map for disaster recovery

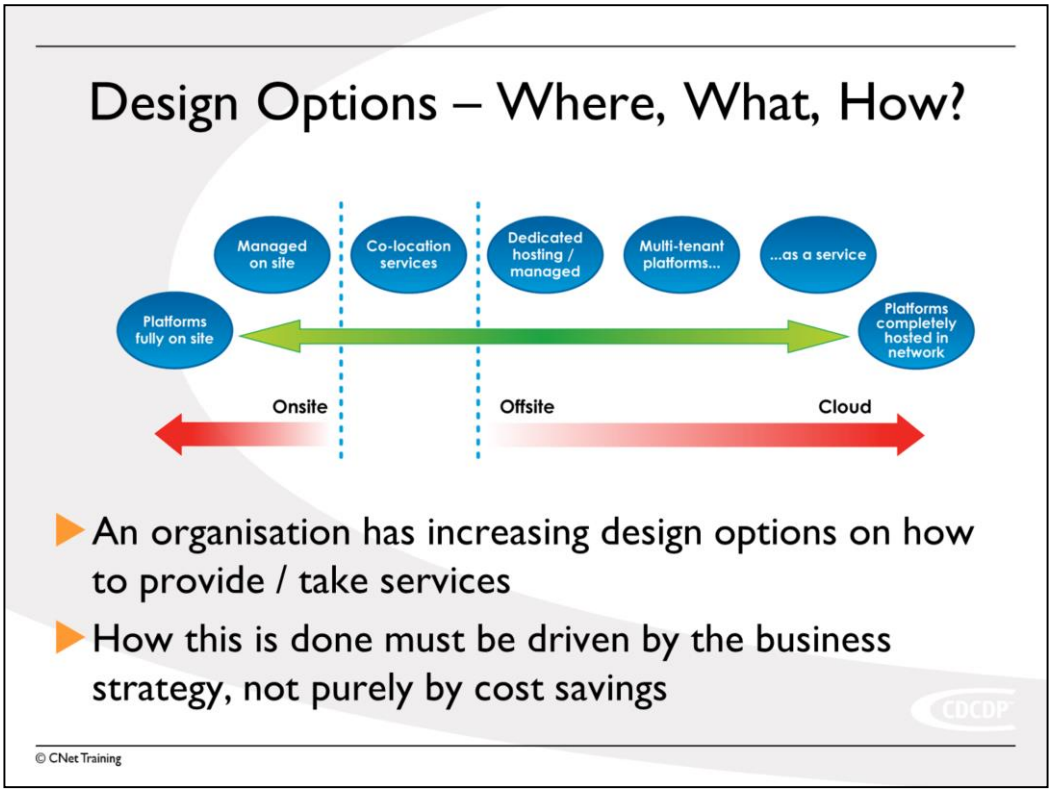


Leveraging third-party computing capability over the network is a good way to cut costs, increase scale, and improve agility. The concept of cloud computing involves a Data Centre somewhere in the world, or even multiple Data Centres scattered around the world. This is a paradigm shift from the historical client-server architecture, where the network users owned, maintained, and operated their own network infrastructure, server rooms, data servers and applications.

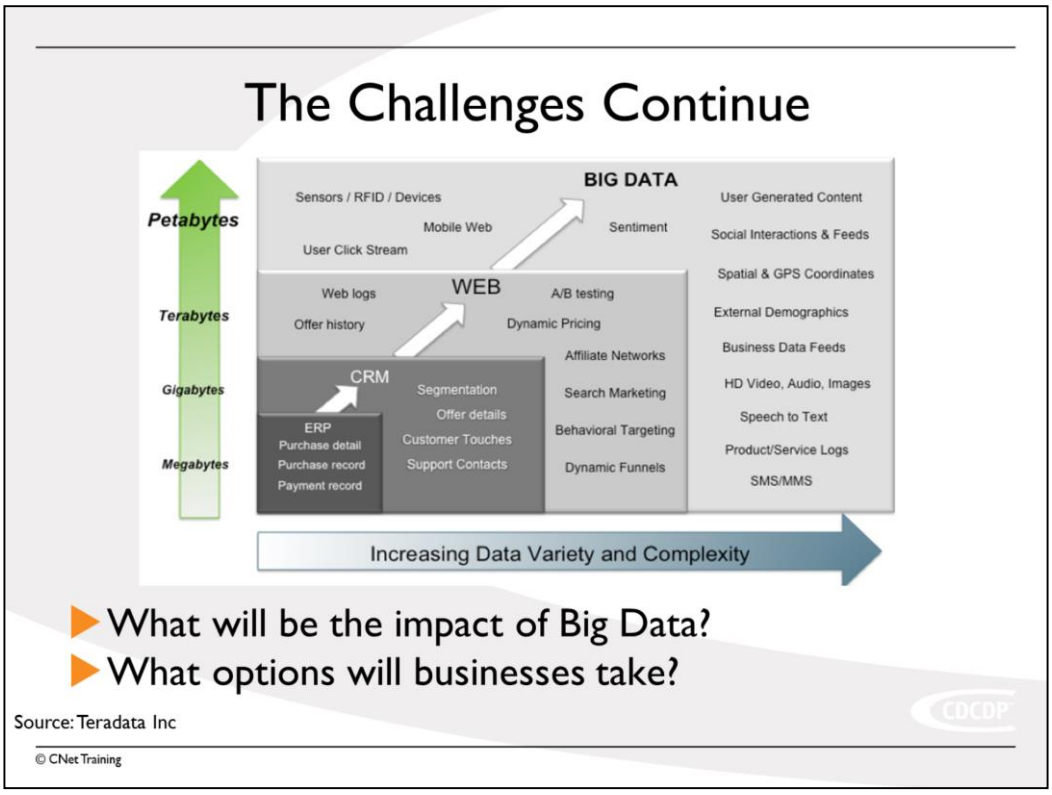
Typical cloud computing providers deliver common business applications online that are accessed from web browsers, while the software and data are stored on the servers or SAN devices. These applications are broadly divided into the following categories:

- Software as a Service (SaaS)
- Utility (Service) Computing
- Web Services
- Platform as a Service (PaaS)
- Managed Service Providers (MSP)
- Service Commerce
- Internet Integration

These Data Centres are hosting the servers and applications the clients use to operate their businesses.



There is an increasing number of design options appearing for businesses to deliver their IT strategies. The choice of enterprise, managed hosting and co-location solutions is being extended by service providers offering offsite solutions including complete solutions hosted in 'the cloud'. The choices made by an organisation have major impacts on the design processes required.



The introduction of Big Data has increased the options open to a business and customer from a business, technical and financial perspective.

Business

- Opportunity to enable innovative new business models
- Potential for new insights that drive competitive advantage

Technical

- Data collected and stored continues to grow exponentially
- Data is increasingly everywhere and in many formats
- Traditional solutions are failing under new requirements

Financial

- Cost of data systems, as a percentage of IT spend, continues to grow
- Cost advantages of commodity hardware and open source software

Review

- Can you?
  - Identify the business need
  - Define a Data Centre
  - Identify the main Data Centre types

© CNet Training

Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

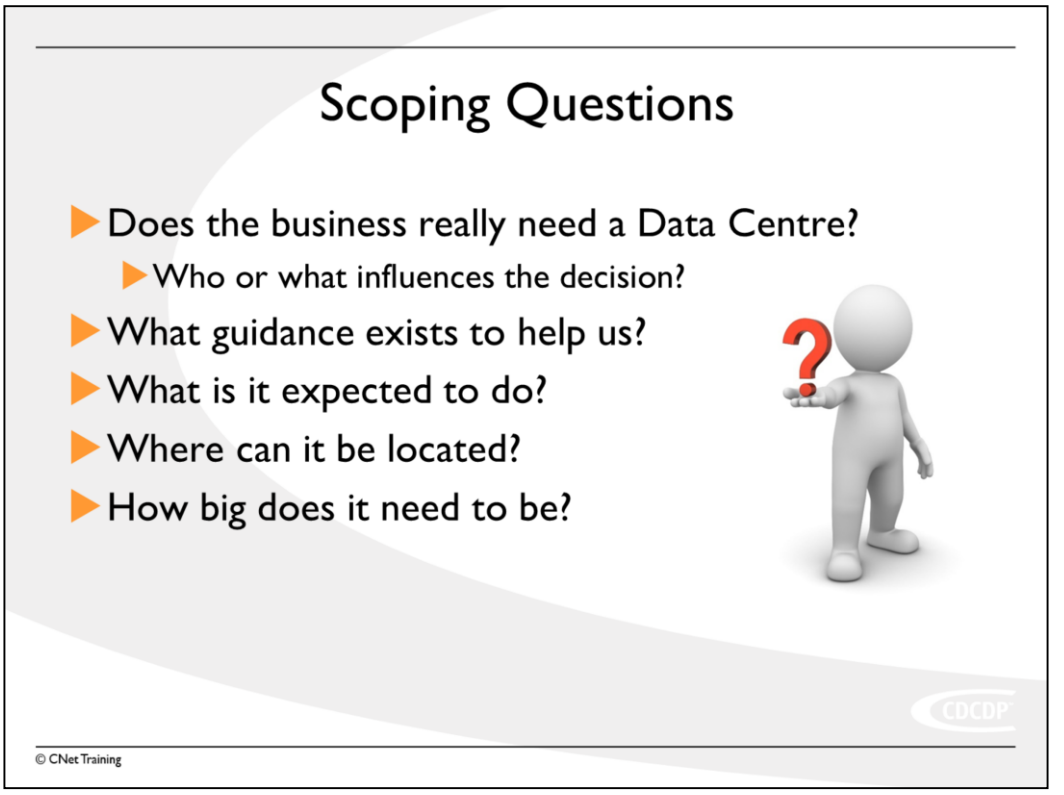
Scoping the Requirement

Version 1509

Objectives

- At the end of this module you will be able to:
  - Review national and international standards
  - Review the Uptime Institute Tier levels
  - Discuss Data Centre location
  - Discuss Data Centre specifications

© CNet Training



As a CDCD, you should never take things for granted, instead we should question our decisions and test them against the knowledge that we will build up throughout our design career.

There are some simple questions that should be asked as a starting point, as it is essential the scoping requirements are properly understood prior to commencing the initial design process.

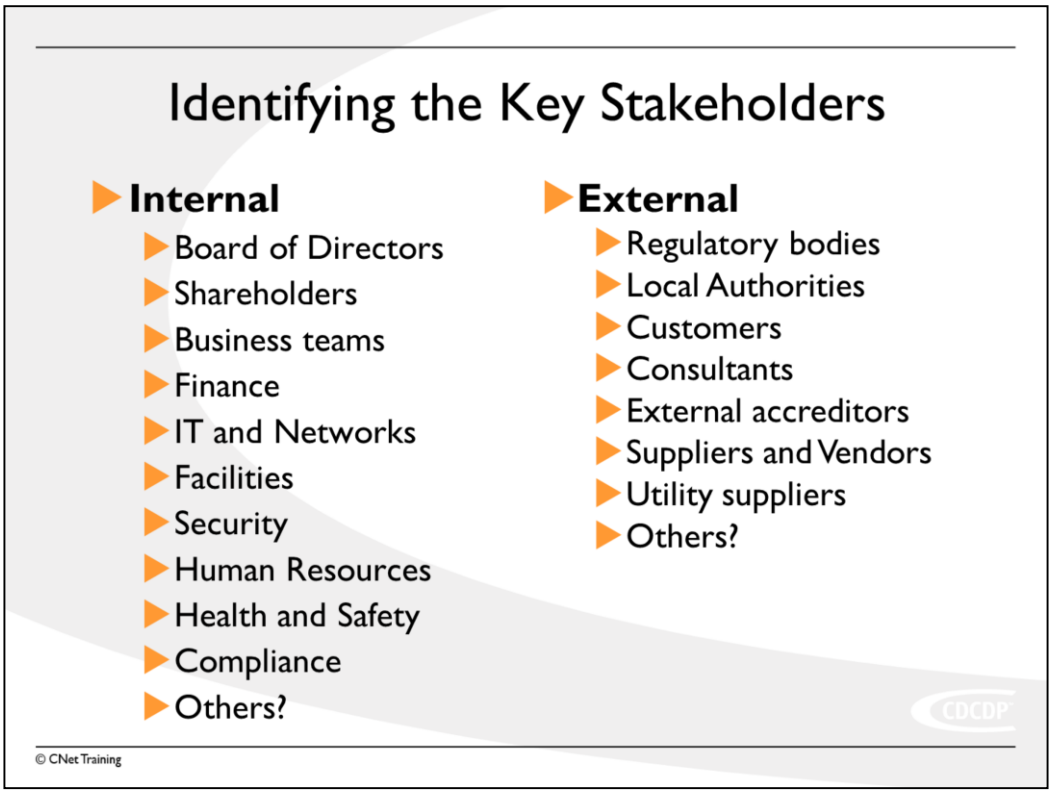
Class Discussion

- Who are the stakeholders involved in determining whether a business needs a Data Centre?

© CNet Training

Considerations:

- Business direction and goals (short-term & long-term)
- The era of expanding co-location / cloud offerings (lower costs, shorter turnaround, greater flexibility)



There are many stakeholders involved, with different needs, requirements and opinions. It is fundamental to the success of the project these are placed within an agreed framework to allow the correct strategic decisions to be made.

It is critical to identify key players and to ensure their requirements are fully considered in the final design. Ownership of systems, processes and procedures should also be considered and agreed upon. It is almost certain there will be different points of view that do not align with the requirements of all parties, so discussion and agreement is vital. Therefore, the CDCD must be involved in the design and planning processes from the very beginning.

Market Drivers

- Growth in on-demand business sector
  - Share dealing, Internet banking, credit card transactions, mail-order, Internet gambling
- More than 5 billion people now calling, texting, tweeting or browsing on mobile phones (Source: sas)
- Increased demand for Cloud computing, with global market increases of 10% projected for 2014-2018 (Source: Research and Markets)
- Remote workers and 'follow the sun' operations
- Business growth leading to storage growth, Big Data and virtualisation are now key drivers (Source: datacentres.com)
- Corporatism requiring security, storage, resilience and backup

© CNet Training

There are many reasons businesses are going down the Data Centre route, but in some respects it is a return to the way things were done previously. Until the 1990s, the majority of key IT systems were running on mainframes or mini-computers which were administered centrally in a business. It was not until the mid-1990s that client-server workloads became the major player. Whilst offering great flexibility, this also brought about increased problems in managing the distributed IT systems.

As businesses started to rely almost totally on IT systems for critical data, the need for resilience and security became paramount. This was a real problem for distributed systems.

At the end of the 1990s (and accelerating in the early part of this century) we saw the growth of 'on demand business workloads', where the demand could vary dramatically depending on business activity. So a managed, dynamically-scalable solution was needed. Hand-in-hand with this we have seen the demand for data storage going 'through the roof' and forecasted to continue with 'Big Data' becoming more prominent.

Concerns about climate change have focused attention on the power efficiency of the Data Centre and the economic crisis has raised cost issues. However, the requirement for the service they provide remains. This has caused the Data Centre community to think about how to provide services and yet meet the many demands and constraints they face, whilst continuing to support business needs.

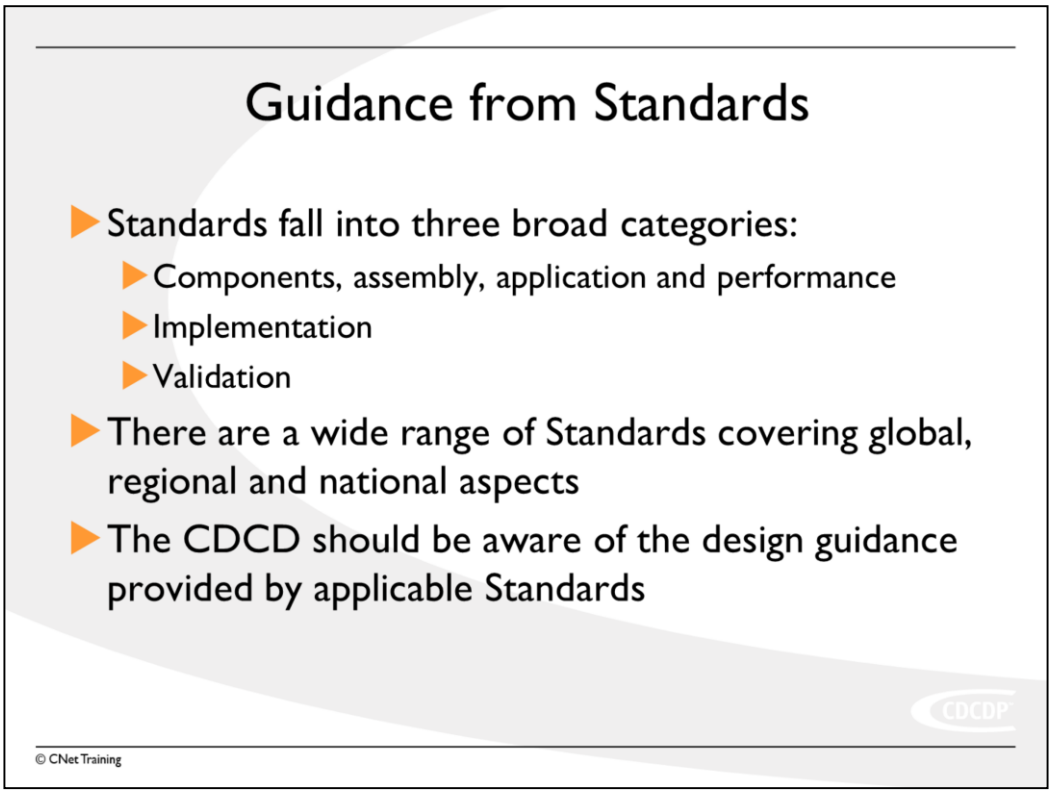
Political Drivers

- Disaster recovery and backup
  - USA - 9/11, Hurricanes Katrina and Sandy
  - UK - 7/7, Buncefield Oil Depot
- Data protection legislation
  - Sarbanes-Oxley, Basel III, PCI-DSS, Cybersecurity
- Data retention directives
  - EU Directive (Aug. 2007), retention of call detail records (CDRs) from 6 months to 2 years
  - US Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act (2009), 2 years of call records
- Civil contingencies acts
- Carbon reduction initiatives
  - Kyoto, Copenhagen, Climate Change Agreements (CCA)

© CNet Training

The critical nature of electronic data was highlighted by some disasters. The cost of lost data has been tremendous and led to legislation trying to stop it happening again. The legislation comes from many different angles, including:

- Disaster recovery after natural events
- Financial and corporate compliance after a number of high profile failures
- Anti-terrorist contingencies
- Carbon Reduction requirements driving towards the Kyoto Accord and other similar initiatives
- PCI - DSS - Payment Card Industry - Data Security Standard
- Basel III - International banking laws and regulations



A Standard is best viewed as a minimum set of requirements to meet a certain defined performance. Standards vary between countries for a number of reasons, often historical. Whilst there is ongoing harmonisation between Standards, this is by no means complete, and it is important country-specific Standards are considered in the design. Standards are considered to be living documents, as they are undergoing a continual development process.

Therefore, the efforts to ensure harmonisation between Standards and regulations prevalent within different disciplines does not necessarily guarantee all of the unique requirements for a specific engineering design are covered.

Standards are something a CDCD cannot afford to ignore for both legal and best practice applications. All relevant standards and procedures should be referenced within the processes and procedures that support the business and operational strategy. Applying standards will ensure:

- The business and personnel clearly understand legal legislation.
- Continual maintenance of current industry approved practices.
- Safe working practices are maintained.
- A common language for demonstrating competence in a competitive market.
- A useful reference to compare a data centre performance against recognised industry benchmarks.
- An understanding of new concepts.

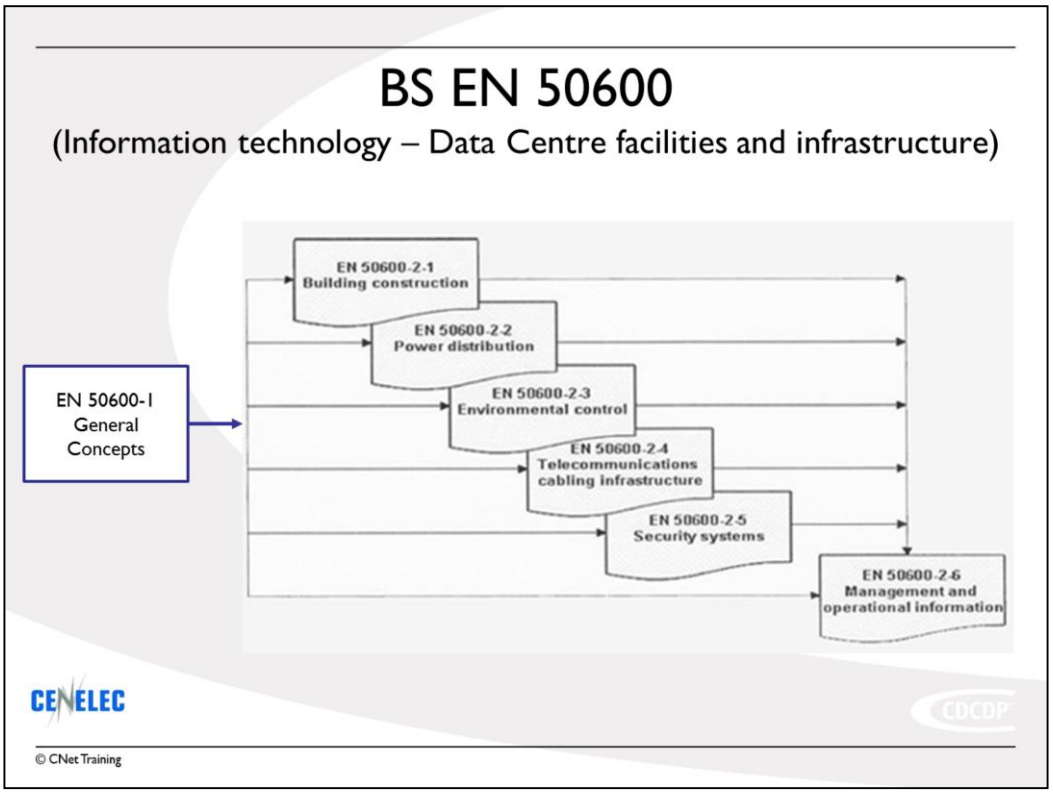
- ANSI – American National Standards Institute
- BSI – British Standards Institution
- BICSI – Building Industry Consulting Services International
- CSA – Canadian Standards Association
- CENELEC – European Committee for Electrotechnical Standardization
- IEC – International Electrotechnical Commission
- IEEE – The Institute of Electrical and Electronic Engineers
- ETSI – European Telecommunications Standards Institute
- ISO – International Organisation for Standardisation
- Standards Australia
- TIA – Telecommunications Industry Association

Data Centre-Specific Standards

- BS EN 50600 - Information technology – Data centre facilities and infrastructure
- BS EN 50173-5 – Information technology – Generic cabling systems – Part 5: Data centres
- TIA 942-A – Telecommunications Infrastructure Standard for Data Centers
- ISO/IEC 24764 - Information technology - Generic cabling systems for data centres
- BICSI 002 - Data Center Design and Implementation Best Practices

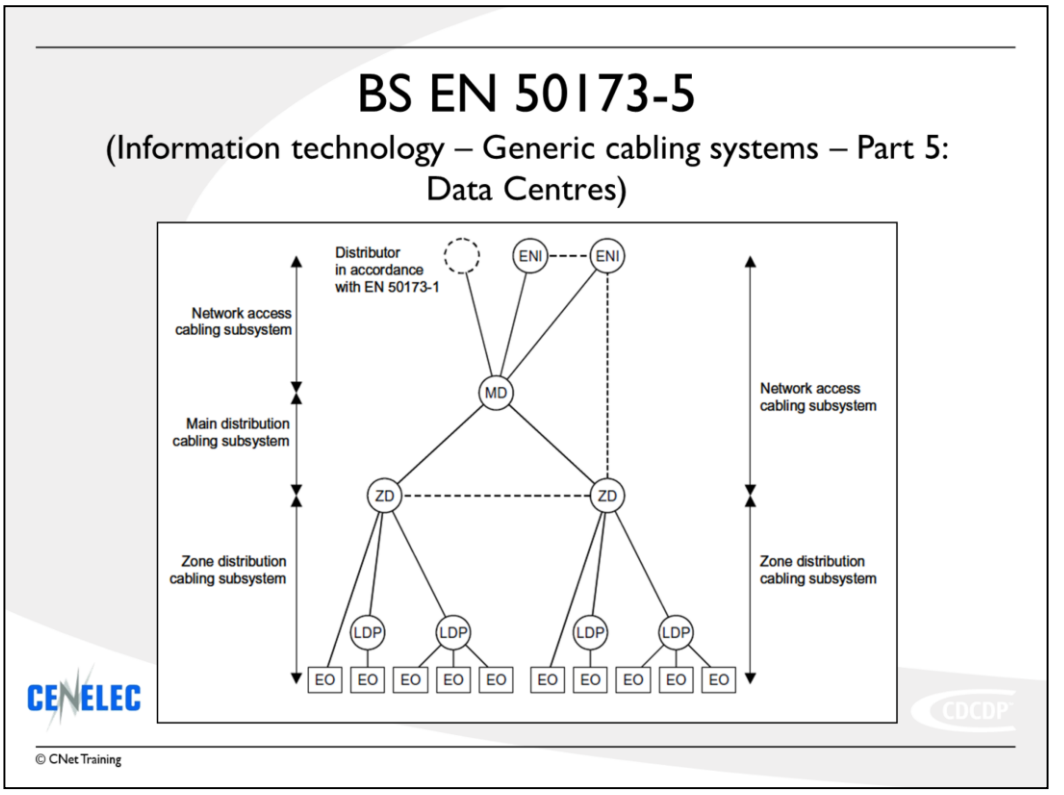
© CNet Training

These Standards cover specific aspects within various Data Centre environments, and will be cross referenced during forthcoming modules.



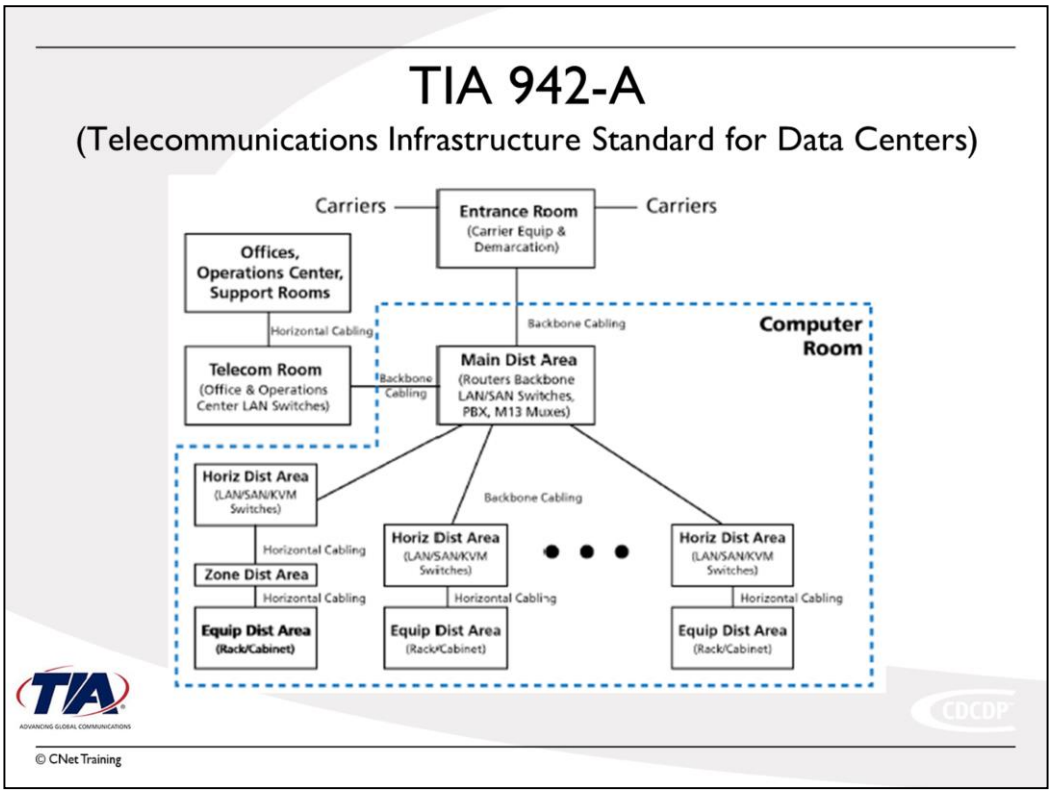
The scope of this Standard:

- Details issues to be addressed in a business risk and operating cost analysis, enabling application of an appropriate Data Centre classification
- Defines the common aspects of Data Centres, including terminology, parameters and reference models (functional elements and their accommodation) addressing both the size and complexity of their intended purpose
- Describes general aspects of the facilities and infrastructure required to support effective operation of telecommunications within Data Centres
- Specifies a classification system, based upon the key criteria of 'availability', 'security' and 'energy efficiency' over the planned lifetime of the Data Centre, for the provision of effective facilities and infrastructure
- Describes the general design principles for Data Centres upon which the requirements of the EN 50600 series are based, including symbols, labels, coding in drawings, quality assurance and education



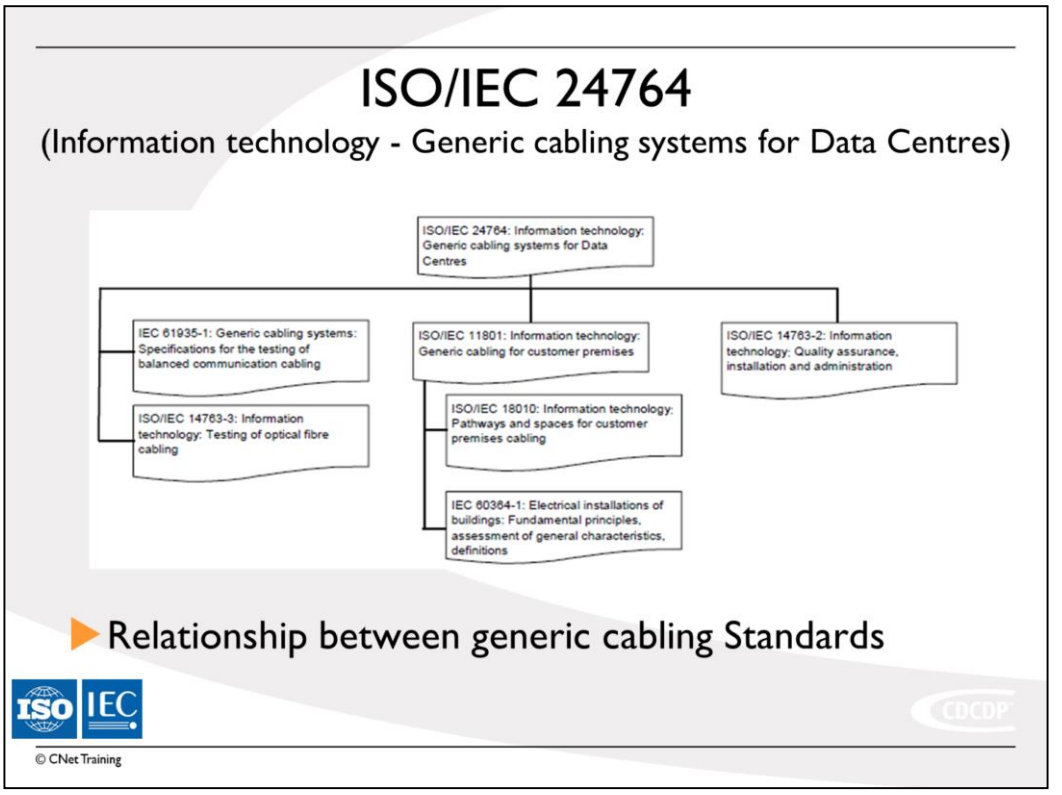
BS EN 50173-5, provides:

- Users with an application-independent generic cabling system and an open market for cabling components
- Requirements for infrastructures supporting critical applications within Data Centres
- A flexible cabling scheme, so that modifications are both easy and economical
- A scalable structure to support expansion with minimum operational disruption
- Building professionals 'for example, architects' with guidance allowing the accommodation of cabling before specific requirements are known. This could be during initial planning for either construction or refurbishment
- Industry and standardisation bodies with a cabling system which supports current products, and provides a basis for future product development and applications standardisation.



This Standard specifies requirements for Data Centre and telecommunication infrastructure, including single tenant enterprise Data Centres and multi-tenant Internet hosting Data Centres. Specifications are provided from very small Data Centres, to Data Centres occupying multiple building floors or rooms. The content incorporates:

- Data Centre design overview
- Data Centre cabling system infrastructure
- Data Centre telecommunications spaces and related topologies
- Data Centre cabling systems
- Data Centre cabling pathways
- Data Centre redundancy
- Annexes addressing cabling design considerations, access provider information, coordination of equipment plans with other engineers, Data Centre site selection and building design considerations, Data Centre infrastructure levels, and Data Centre design examples



ISO/IEC 24764 specifies generic cabling supporting a wide range of communications services for use within a Data Centre. It covers balanced cabling and optical fibre cabling. It is based upon and references the requirements of ISO/IEC 11801, and contains additional requirements appropriate to Data Centres.

This international Standard provides:

- Data Centre users with an application-independent generic cabling system capable of supporting a wide range of applications
- Data Centre users with a flexible cabling scheme allowing easy and economical modifications
- Data Centre professionals with guidance that accommodates cabling before specific requirements are known; that is, in the initial planning either for construction or refurbishment
- Industry and applications standardisation bodies with a cabling system supporting both current products and a basis for future product development

BICSI 002

(Data Center Design and Implementation Best Practices)

- BICSI 002 covers the main design and best practices for:
  - Power
  - Cooling
  - Cabling and IT
  - Site
  - Building
  - Security

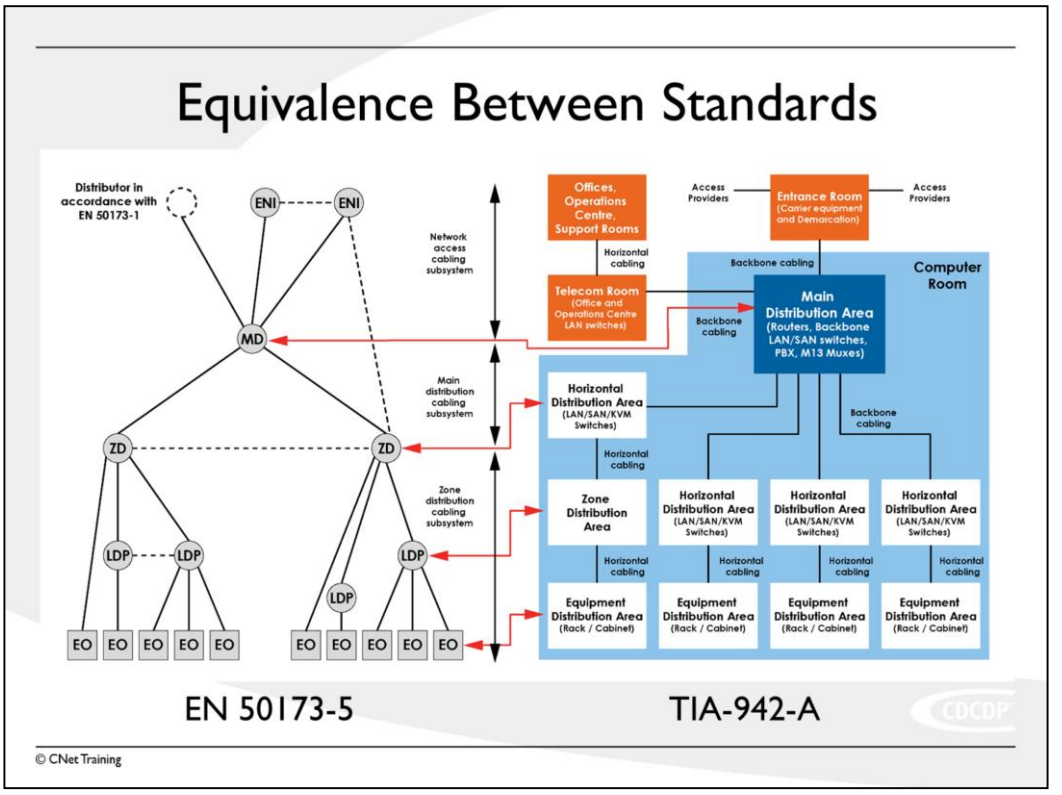
Bicsi

CDCDP

© CNet Training

BICSI 002-2014 contains requirements, recommendations, and additional information that should be considered when planning and building a Data Centre, such as site selection, layout, thermal systems, and security. It is also designed to complement the other industry-recognised Standards. One area that differs is BICSI 002 refers to *classes* as opposed to tier *classifications*.

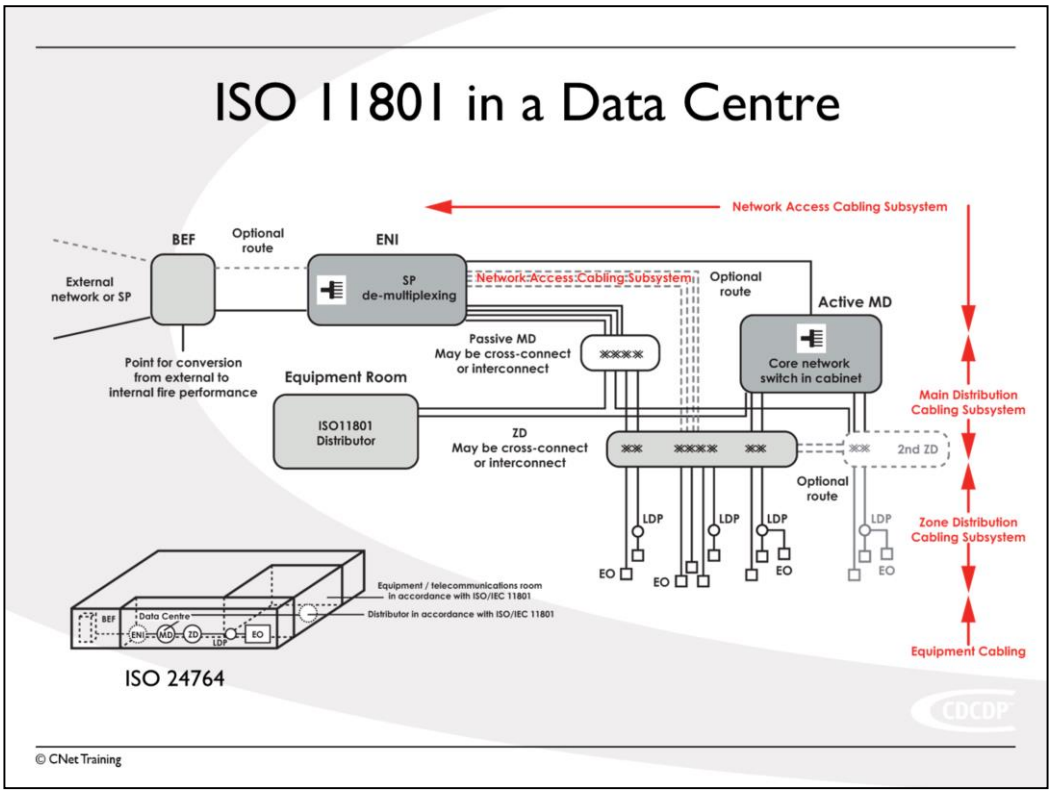
- F0 – No supplemental equipment
- F1 – Some supplemental equipment
- F2 – Critical component redundancy
- F3 – Critical and non-critical component redundancy
- F4 – System redundancy with component redundancy



This demonstrates how terminology can be different between Standards in other parts of the world. It is important the CDCD is familiar with the ones he/she needs for his/her country.

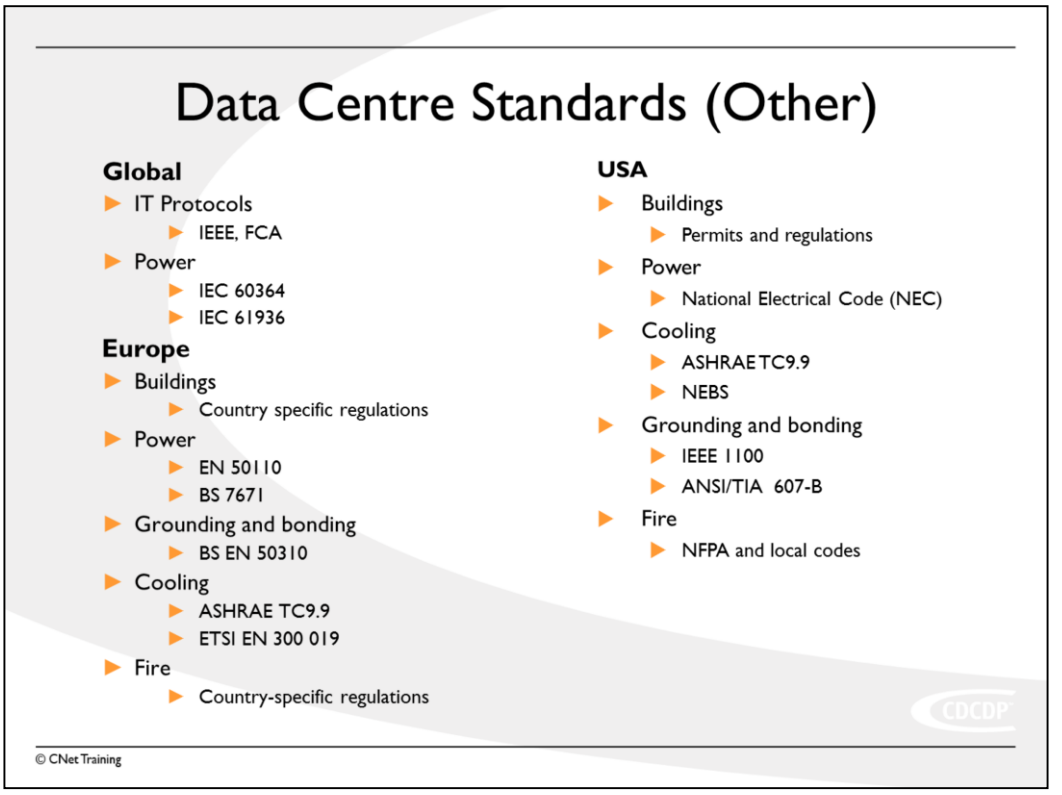
Data Centre cabling infrastructure recommendations from various standards follow the traditional hierarchical star topology, with the usual distance limitations placed on different subsystems.

It is useful to look at the Standards and read the descriptions of the different areas. TIA 942-A identifies physical spaces in the Data Centre, EN 50173-5 discusses performance of the connectivity.



This demonstrates how another Standard refers to the same cabling systems, reinforcing the idea that the CDCD needs to be aware of the similarities and differences. ISO 11801 contains this schematic diagram which shows the topology and physical arrangement of the different subsystems in the Data Centre space.

More and more, the building entrance facility's purpose is to convert from external to internal fire performance cabling. There is an increasing tendency for the demarcation point to be presented closer to the equipment, and for the service provider to be responsible up to the point of use; this will be covered by a service level agreement (SLA). As a result, the entrance facility may actually not exist as a room, but may be inside a separately routed cabinet in the computer room.



Since other industries may be involved in Data Centre design, the CDCD should also be knowledgeable about the related Standards, local and national regulations appropriate to the region.

Worldwide

- IEC 60364 and 61936 contain common rules for electrical installations.

Europe

The European Standard EN 50110 'Operation of Electrical Installations' consists of two parts:

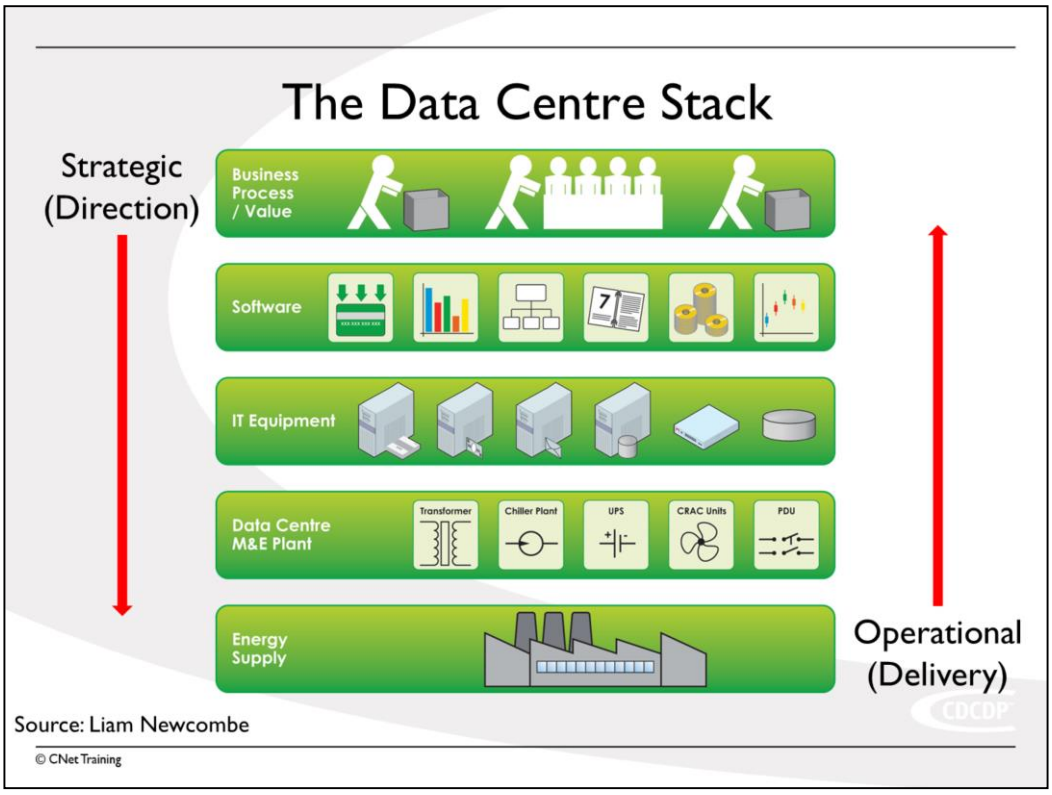
- EN 50110-1 contains minimum requirements valid for all CENELEC countries and some additional informative annexes dealing with safe working.
- EN 50110-2 is a set of normative annexes (one per country) which specifies either the present safety requirements, or provides the respective national supplements to these minimum requirements.
- BS 7671 is the country variant for the UK which ensures compliance with the IEC and EN standards.

USA

National Electrical Code (NEC), National Fire Protection Association (NFPA) Codes and local codes apply. The CDCD needs to keep abreast of the latest discussions regarding codes and standards as they can often be wrongly (and expensively) applied. NEC 645 and NFPA 75 do not apply to all IT facilities, and may or may not apply to the new Data Centre, so the designer must determine the applicable codes at the outset.

American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) standards: Note that the ASHRAE is also commonly quoted in Europe as a 'Standard' for Data Centres.

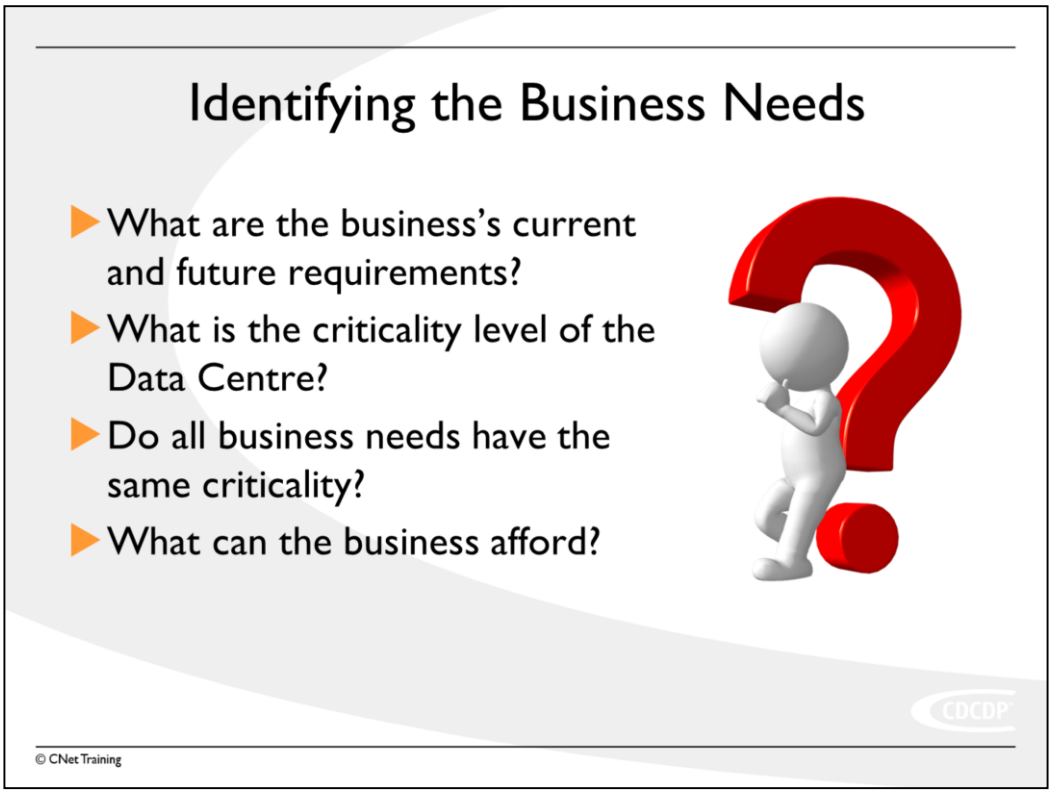
FCA - Fabric Control Application



Let's remind ourselves again of what Data Centres are trying to achieve:

We start off by sourcing energy from a supply. This energy is then delivered through the mechanical and engineering (M&E) plant to the IT equipment, which runs the application software supporting the business activities that the Data Centre drives.

The physical Data Centre exists to deliver the IT strategy of the business. The security of the IT process depends to a high degree on the physical resilience of the Data Centre energy supply and the M&E plant keeping the IT equipment up and running.

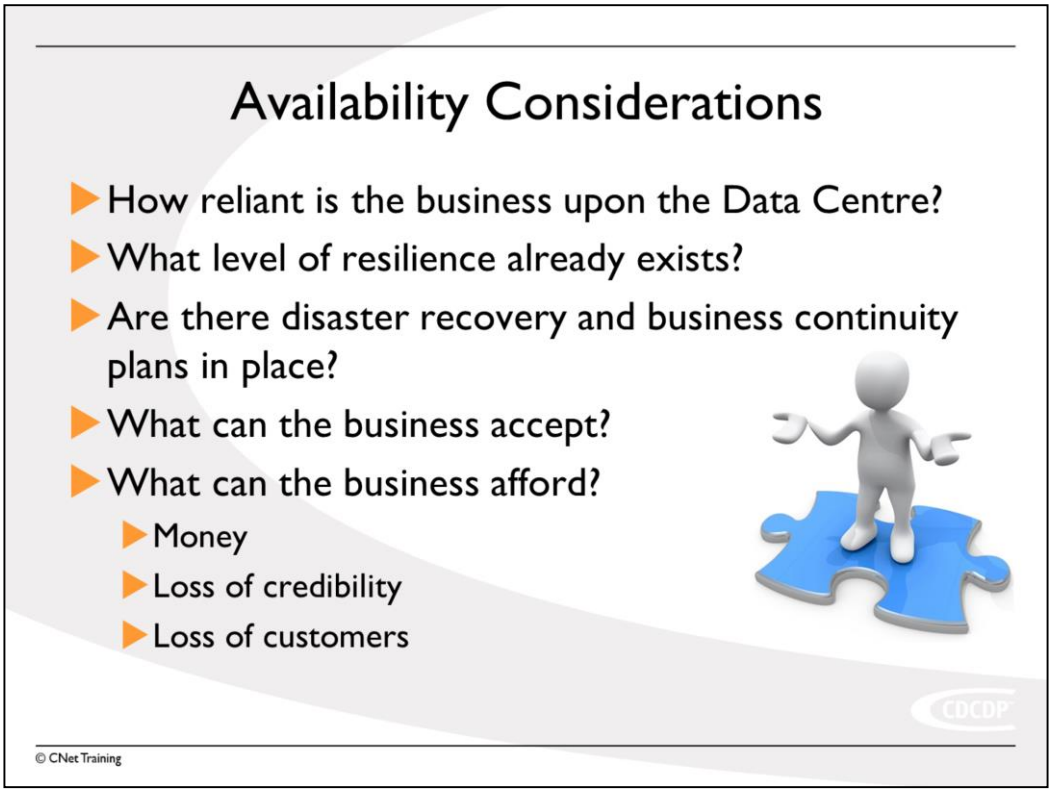


The business need is the prime factor - what does the business expect to get out of the Data Centre? It would be good if a business actually knew what they expect, but it is difficult (or impossible) to guess the future, and many businesses do not even have a clear picture of today's requirement.

Businesses are now starting to differentiate between the processes which make them unique and those which are commodities, and are giving them different levels of treatment in the Data Centre.

Getting the initial scope wrong, or attempting to fulfill false expectations or unrealistic requirements, can be, and very often is very costly.

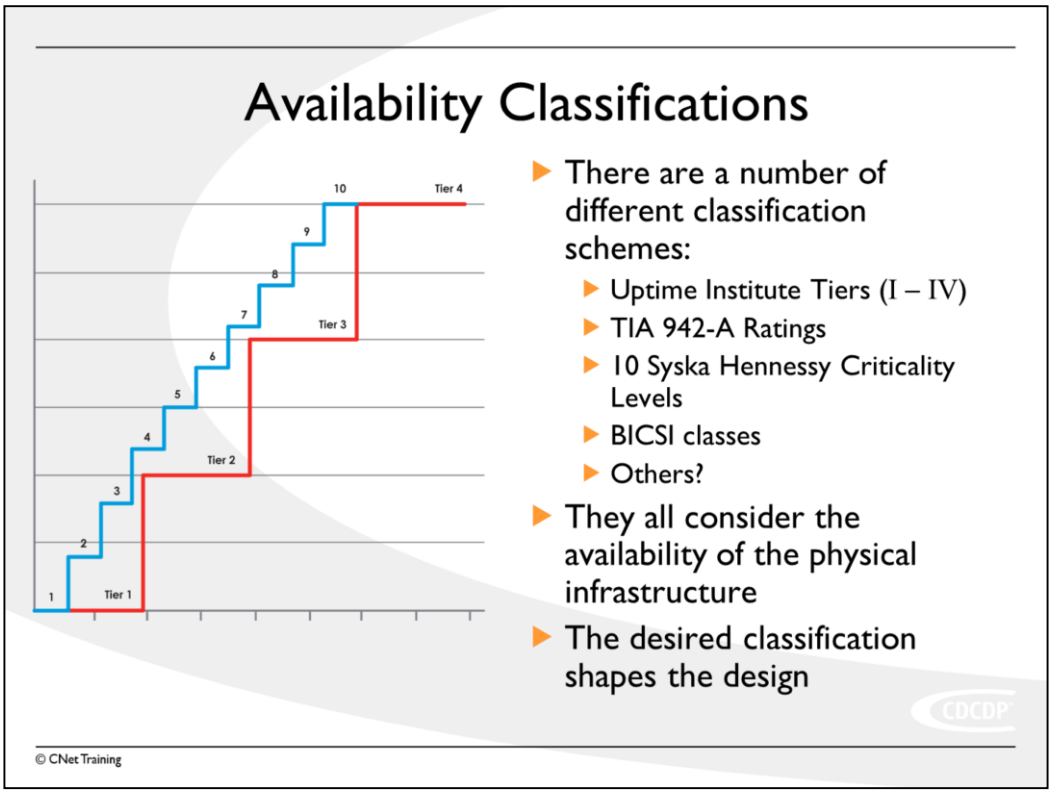
The budget is another prime factor: What is the business able to spend on it? This may be a prime factor in deciding between available options. It is important these factors are understood and dealt with at the early stages by involving all key stakeholders.



It is generally considered that both user and application requirements are the main drivers behind the reliability of the Data Centre.

Terminology and definitions

- **Reliability** - The probability that a component or system will perform as intended over a given period of time.
- **Fault tolerant** - The attribute of a concurrently maintainable and operable system, or facility where redundancy is not lost during failure or maintenance activity.
- **Redundancy** - The provision of secondary components that either become instantly operational or are continuously operational, so in the event of a primary component malfunction, the result will not be mission failure.



During the 1980s, Data Centre operators did not have the resources to help them determine the levels of reliability for their facility. The Site Uptime Network® was formed in 1993 by The Uptime Institute with a clear purpose to directly address and resolve issues affecting continuous site infrastructure (cooling and electrical environment) availability.

Since then, various organisations have developed ways of classifying Data Centres. The Uptime Institute has a longstanding classification based upon four Tiers, TIA 942-A their own specific version, BICSI has Classes, TIA has Ratings and Syska Hennessy has an extended and, it is claimed, more inclusive classification based on 10 Criticality Levels. There are other classifications in use as well, which try to balance criticality against cost.

Whichever classification we choose, when we look at physical systems and infrastructure, there are four common levels of component provision to consider in practice:

- **N**: Only the number of components needed is provided, there is no resilience and any component failure will cause downtime.
- **N+1**: Where the number of components provided is one more than the number (N) of components needed.
- **2N**: Comprises two complete systems, each containing N components, and are run in parallel to hot swap between each other.
- **2(N+1)**: Comprises two N+1 systems in parallel. One side can be taken down for maintenance and the other side will be protected from exposure to the risk of downtime by its own redundant module.

When considering the configuration of systems to achieve the desired reliability levels, it is a good idea to balance redundancy with simplicity.

Uptime Institute Tier Classifications

- Uptime Institute developed an availability Tier rating system to define a facility's performance parameters
- There are four Tier classifications
- The overall tier rating of any Data Centre facility is based upon the lowest rated component
- The location could be the weakest link, and the highest risk

Uptime Institute™

CDCDP

© CNet Training

Determining the actual Uptime Institute Tier classification of a site for design topology is a logical process, although it is often done incorrectly. The Tier topology classification for the whole site is limited by the Tier rating of the weakest subsystem that impacts operations. For example:

- Site has a robust Tier IV uninterruptible power supply (UPS) configuration
- Site also has a Tier II configured chilled water system
- Resulting site rating is Tier II

Certification of a facilities Tier level can only be performed by Uptime Institute.

Uptime Institute Tier Classifications

- Tier I — A single path Data Centre
- Tier II — A single path Data Centre with redundant components
- Tier III — A concurrently maintainable and operable Data Centre
- Tier IV — A fault-tolerant Data Centre

Uptime Institute™

CDCDP

© CNet Training

- **Tier I**: Basic Data Centre that has non-redundant capacity components and a single, non-redundant distribution path to serve the computer devices.
- **Tier II**: This rating of Data Centre has redundant capacity components with a single, non-redundant distribution path to serve the computers.
- **Tier III**: This is a concurrently maintainable facility, with redundant capacity components and multiple independent distribution paths serving the computers, although generally only one distribution path is operational at any time.
- **Tier IV**: Fault-tolerant facility with multiple, independent, physically-isolated systems each with redundant capacity components and multiple, independent, diverse, active distribution paths to the computer devices.

Tier Levels and Availability

- Tier I – 99.671%
- Tier II – 99.741%
- Tier III– 99.982%
- Tier IV– 99.995%
- Actual availability figures can be quite different
- These include an estimate for maintenance outages
- Quality of design, equipment selection and connectivity are critical
- Maintainability and operational procedures have a major impact

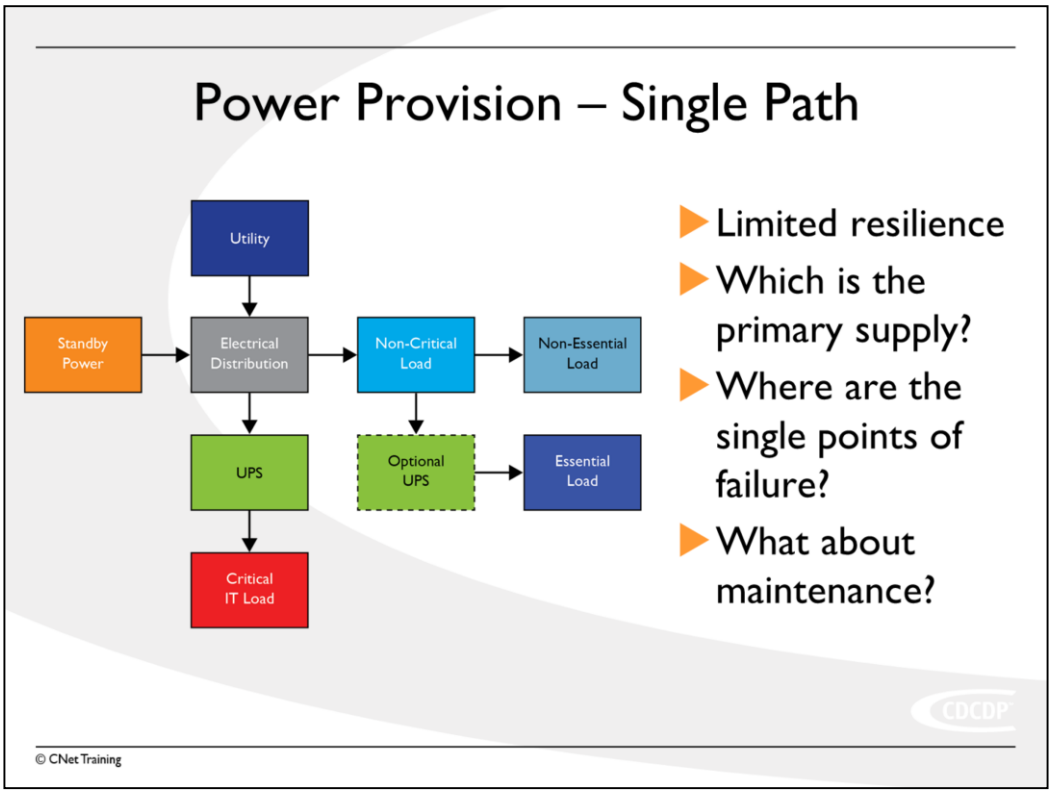
© CNet Training

The stated availability figures are an indication only. In practice, it is easy to find alleged Tier IV Data Centres which fall short of the expected figures. Equally, there are many Tier II Data Centres which easily surpass them. There are many reasons for this - from choice of quality equipment, through to the routing and maintainability of the cabling system. Overly complex designs increase the possibility of human error and are a big issue in practice.

Class Discussion

- What sort of questions can assist in determining the availability required from the Data Centre?
  - Try and imagine how tiers might apply to something like a family car?

© CNet Training

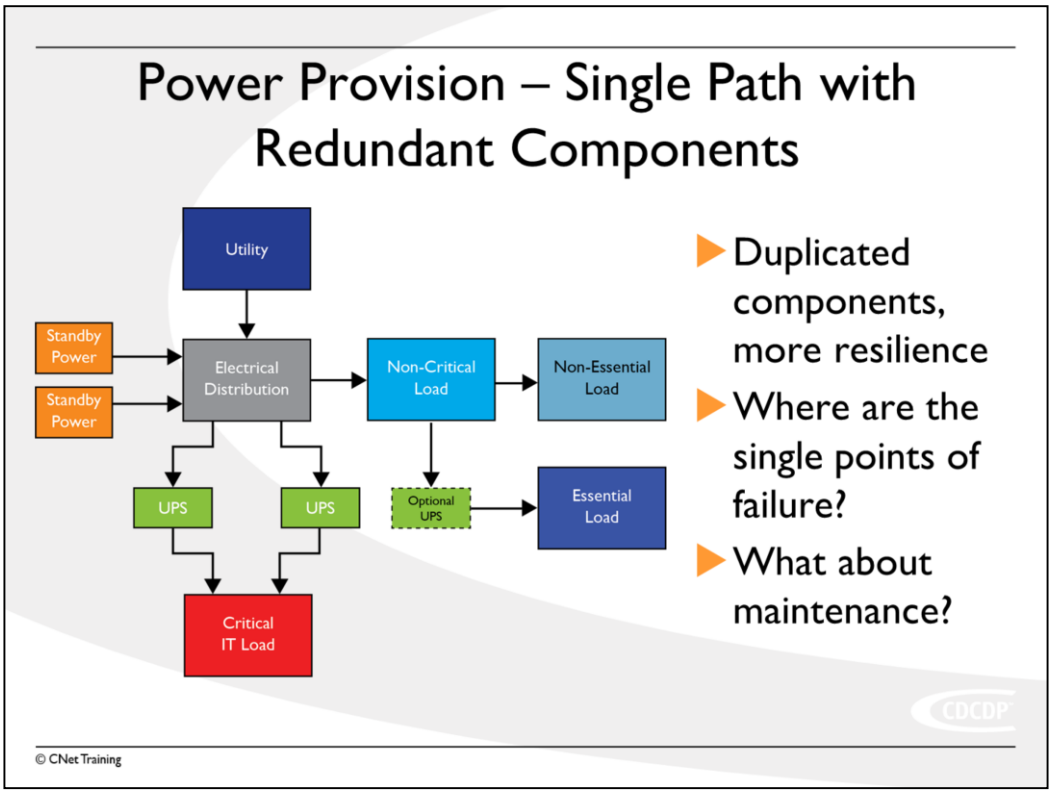


Basic Data Centre with non-redundant capacity components and a single non-redundant distribution path serving the computer equipment. This distribution path incorporates:

- A main electrical supply from the utility.
- A distribution network to split the critical load from the non-critical load. The common belief here is the critical load *is* the IT load, and everything else is non-critical. We shall see later this is not always the case.
- A UPS of some description to ensure the supply to the critical load is maintained.
- A standby system (usually a generator) to replace the utility supply in the case of a power failure.
- Consider the single points of failure that would cause the Data Centre to become unavailable.
- Planned maintenance work will require most or all of the facility infrastructure systems to be shut down, impacting computer operations.

A basic tier description can lead to some poor design decisions and large expense. This can be due to lack of detail on each of these items' real risk of failure in a Data Centre, as well as their consequential effect on the business - is the availability of utility power at risk?

The tier classification is used and just as often misused in the Data Centre community. This configuration could be described as a Tier I.

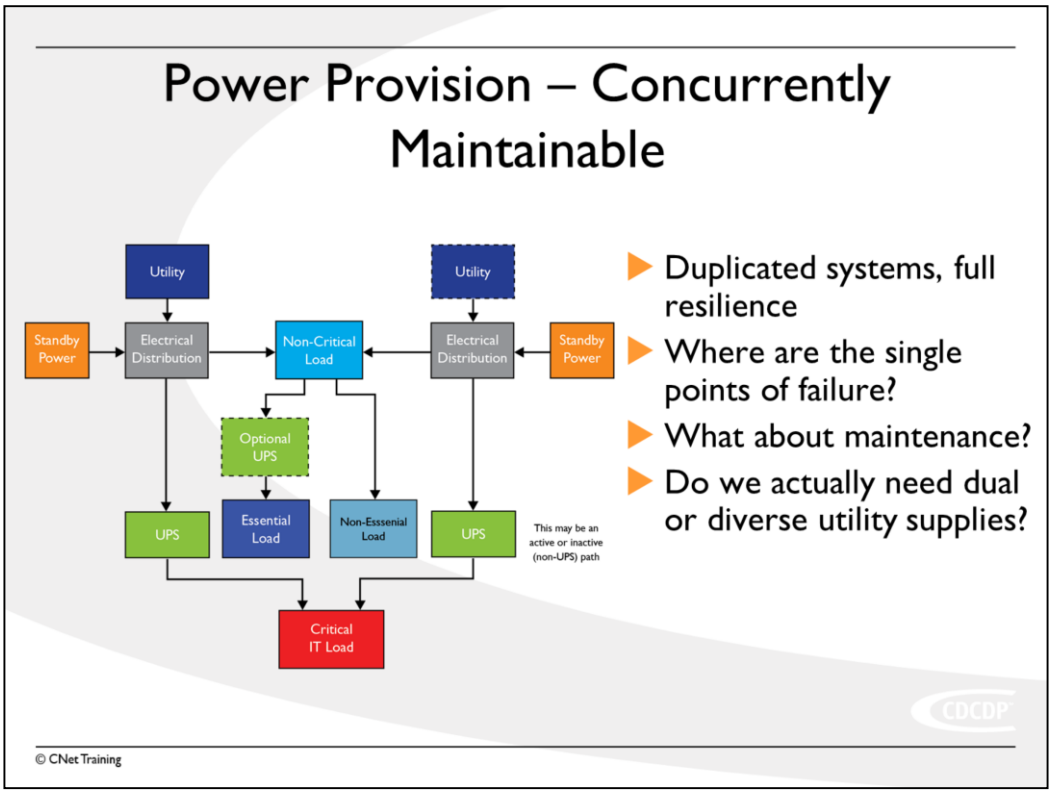


A Data Centre with redundant capacity components and a single, non-redundant path serving the computer equipment. The distribution path incorporates:

- A main electrical supply from the utility.
- A distribution network to split the critical load from the non-critical load. The common belief here is the critical load *is* the IT load, and everything else is non-critical. We shall see later this is not always the case.
- Duplicated UPS of some description to ensure the supply to the critical load is maintained.
- Duplicated standby systems (usually a generator) to replace the utility supply in the case of a power failure.
- Redundant capacity components that can be removed from service on a planned basis without causing shutdown to active IT environments.

The additional capital cost of the duplicated components is self-evident, but there is also an ongoing running cost penalty as the systems are running at low utilisation by design.

This would be Tier II.

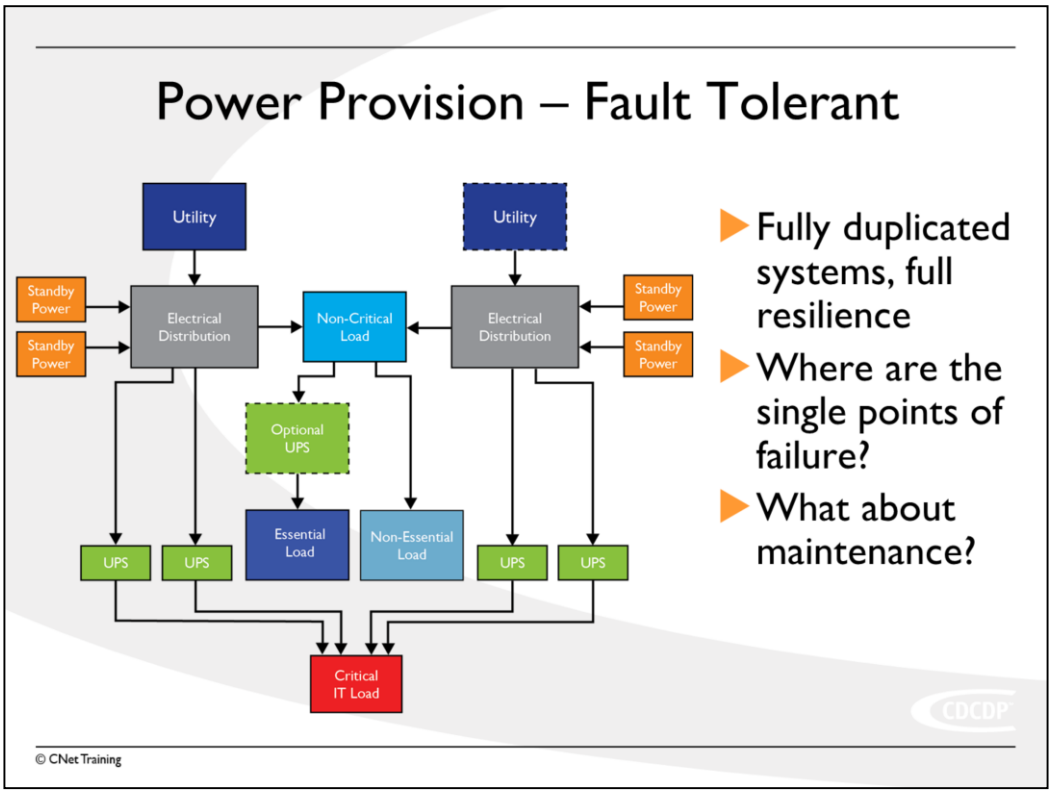


A Data Centre with redundant capacity components and multiple independent distribution paths serving the computer equipment. The distribution paths incorporate:

- Diverse electrical supplies from the utility.
- Duplicated distribution networks to split the critical load from the non-critical load. The common belief here is the critical load *is* the IT load, and everything else is non-critical. We shall see later this is not always the case.
- Redundant UPS of some description to ensure the supply to the critical load is maintained.
- Redundant standby systems (usually a generator) to replace the utility supply in the case of a power failure.
- Any of the capacity components and elements in the distribution paths can be removed from service on a planned basis without impacting active IT environments.
- Only one distribution path is required to serve the computer equipment at any time.

The additional capital cost of the duplicated systems is self-evident, but there is also a very significant ongoing running cost penalty as the systems are running at very low utilisation, by design.

This would be Tier III.



A Data Centre with multiple, independent, physically isolated systems providing redundant capacity components and multiple independent, diverse and active distribution paths simultaneously serving the computer equipment. The distribution paths incorporate:

- Diverse electrical supplies from the utility.
- Duplicated distribution networks to split the critical load from the non-critical load. The common belief here is that the critical load *is* the IT load, and everything else is non-critical. We shall see later that this is not always the case.
- Duplicated UPS of some description in each network to ensure the supply to the critical load is maintained.
- Duplicated standby systems (usually a generator) in each network to replace the utility supply in the case of a power failure.
- The redundant capacity components and diverse distribution paths are configured such that 'N' capacity is providing power and cooling to the computer equipment after any infrastructure failure.
- Each and every capacity component and element in the distribution paths can be removed from service on a planned basis without impacting active IT environments.
- A single failure of any capacity system, component or distribution element will not impact the operation of the computer equipment.
- All components must be compartmentalized.
- There is a requirement for continuous cooling.

The additional capital cost of duplicated systems is self-evident, but there is also a very significant ongoing running cost penalty as the systems are running at very low utilisation, by design.

This would be Tier IV.

Uptime Institute Tier Classification

- There are many other factors that can effect tier classification over the lifetime of the Data Centre:
  - Location
  - Architecture
  - And other key considerations:
    - Redundancy
    - Capacity
    - Expandability
    - Maintainability

Uptime Institute™

CDCDP

© CNet Training

Historically, Tier I facilities have their roots in the mainframe environments of the 1970s whereas, at the other end of the scale, Tier IV facilities became possible with the introduction of computers with dual-power capabilities around the mid-1990s.

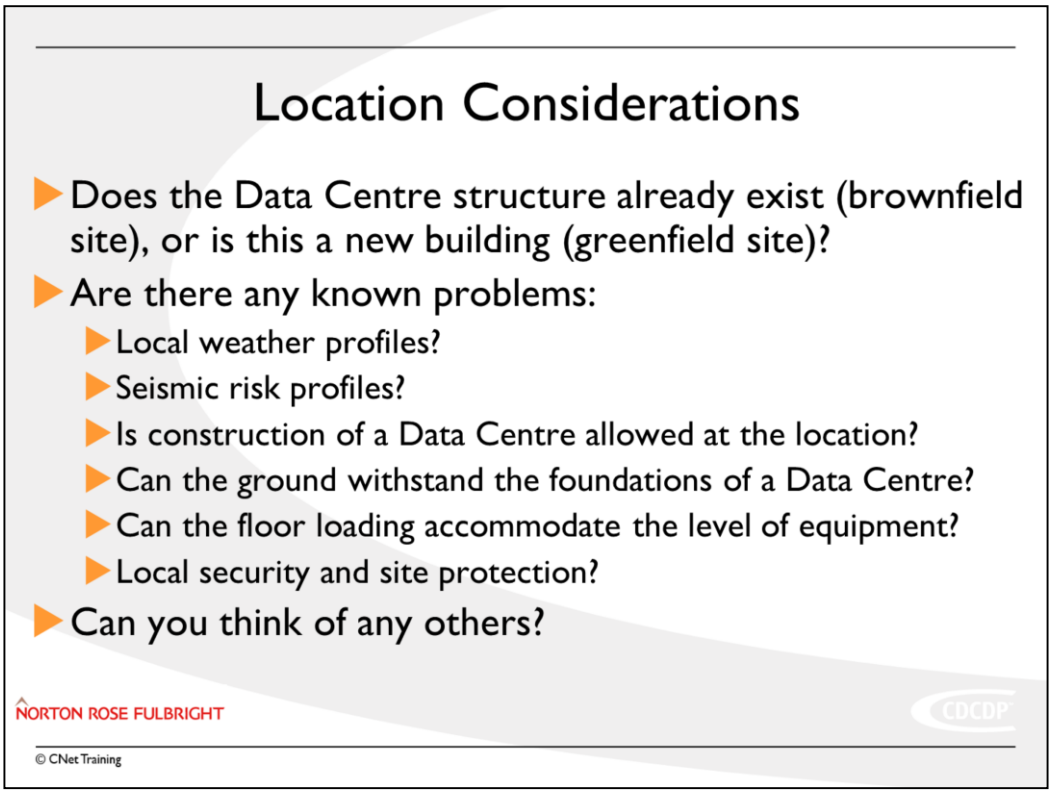
A responsible approach to investment in site infrastructure requires:

- A clear understanding of all facility availability objectives needed to support current and future business requirements
- Consistent design, build, and operation of the site to ensure dynamic conformance to those needs.

Class Discussion

- What sort of questions should the CDCD consider when determining the suitability of the location?

© CNet Training



To coin a well-used adage, the key to Data Centre design is 'location, location, location'. There are of course many factors that will determine the final location of the Data Centre facility. The CDCD should have a good understanding of these factors and how they impact not only the selection of the site, but also how that location may affect the facility's resilience today and into the future.

There are many questions to ask when selecting a site for a Data Centre. Some things are fairly obvious and others are not: Costs of space and power, network latency and lease or buy options all impact site selection.

Can you identify any others that you have encountered?

Location Questions

- The CDCD needs to consider:
  - Is there utility connectivity to mains electrical, gas, water, sewage and telecommunications services? Dual provision?
  - How is the air quality at the location? Is there any risk of IT equipment exposure to dust, industrial by-products, or other contaminants?
  - Is the site located in a market with a population/pipeline of skilled/educated professionals?
  - Are there any future plans to develop the surrounding area?

© CNet Training

The CDCD should always consider the impact of the local environment and available services on the Data Centre. It is always better to ask the utilities: 'This is what I am trying to do, so what can you do for me?' rather than specifying what you need.

Location Recommendations

- Standards offer some guidance, for example:
  - The site should not be located in a 100 year flood plain, near an earthquake fault or downstream from a dam
  - The building should not be on the flight path of any nearby airports
  - The building should be no closer than 800m (½ mile) from a railroad or major highway.
  - The building should not be within 400m (¼ mile) of an airport, research laboratory, chemical plant, landfill, river, coastline or dam
  - The building should not be located in high crime areas
  - The building should not be within 800m (½ mile) of a military base
  - The building should not be within 2km (1½ mile) of a nuclear, munitions or defence plant
  - The building should not be located adjacent to a foreign embassy
  - Electromagnetic compatibility (EMC) risks must be minimised by locating away from radar transmitters and mobile phone masts

© CNet Training

Standards such as TIA 942-A contain a number of recommendations. We do not have knowledge or control of what happens inside other facilities, so we mitigate the potential impact by separation, which can also buy time to react. If there was a disaster, how much area around the incident would emergency services cordon off, and what effects would it have on transport links and access for staff?

Building Considerations

- Standards identify some requirements of the building
  - Ceiling height
  - Floor loading
  - Floor hanging capacity
  - Doors
  - Lighting

© CNet Training

Data Centre Standards provide guidance and recommendations, but local building and fire regulations will take precedence.

Floor Loading

- Floor loading capacity in the computer room shall be sufficient to bear both the distributed and concentrated load of installed equipment with associated cabling and media
- The minimum distributed floor loading capacity shall be 7.2kPa (150lb/sq.ft)
- The recommended distributed floor loading capacity is 12kPa (250lb/sq.ft)

Source: TIA 942-A

© CNet Training

Data Centre equipment can be very heavy, with some cabinets being designed to support up to 1.5 ton (1,500 Kgs/3,300 lbs). Therefore, another obvious requirement of the building is that the floor must be strong enough.

TIA 942-A and other Standards recommend floor loading capacities in the different Data Centre spaces in the computer room; the floor should be capable of withstanding a distributed load of 12kPa (1221Kg/m³ or 250lb/sq.ft). Floor loading has a high risk impact and should be discussed fully with the structural engineer.

It should be noted these are actually baseline figures, and more precise floor loading figures can be found in:

- TIA 569B – Commercial building standard for telecommunication pathways and spaces
- BS EN 12825 – Raised access floors

Floor Hanging Capacity

- The floor shall also have a minimum of 1.2kPa (25lb/sq.ft) hanging capacity for supporting loads suspended from the bottom of the floor (e.g., cable ladders suspended from the ceiling of the floor below)
- The recommended hanging capacity of the floor is 2.4kPa (50lb/sq.ft)

Source: TIA 942-A

© CNet Training

If the floor is a raised floor, it must be able to support equipment hanging below it, as well as equipment on top of it.

Doors

- Doors shall be a minimum of 1m (3ft 3 in) wide and 2.13m (7ft) high, without doorsills, hinged to open outward, slide side-to-side, or be removable
- Doors shall be fitted with locks and have either no centre posts, or removable centre posts to facilitate access for large equipment
- Exit requirements for the computer room shall meet the safety/emergency requirements of the local authority having jurisdiction (AHJ)

Source: TIA 942-A

© CNet Training

Another obvious requirement is the ability to get equipment in or out of the Data Centre. This can be a problem where Data Centre access is via other parts of the building.

As the Data Centre is a secure environment, it should go without saying the doors should be secured with a suitable grade of lock. If the doors form part of the emergency exit route, they must comply with local codes.

Lighting

- Level 1: Data Centre unoccupied – Lighting should be sufficient to allow effective use of video surveillance equipment
- Level 2: Initial entry into the Data Centre – Motion sensors should be used to activate lights in the immediate area of entry, and be programmed to illuminate aisles and passageways.
- Level 3: Occupied space - Lighting shall be a minimum of 500 Lux in the horizontal plane and 200 Lux in the vertical plane, measured 1m (3ft 3in) above the finished floor in the middle of all aisles between cabinets

Source: TIA 942-A

© CNet Training

A Data Centre is not a workplace, but work is carried out under controlled procedures. It is important it is well lit when work is being carried out. This is an area where many Data Centres fail to meet the standard.

The CDCD and the electrical engineer need to work together to ensure the luminaire positions align with the rack layout in order to meet these requirements. This simply requires co-ordination and co-operation.

Note: 1 foot candle = 10 Lux

Ceiling Height

- The minimum height in the computer room shall be 2.6m (8ft 6in) from the finished floor to any obstructions, such as sprinklers, lighting fixtures or cameras (Source: TIA 942-A)
- Many Data Centres are built with greater 'slab-to-slab' clearances. However, there are two design factors that may impact the height of the ceiling:
  - The cooling architecture may have a significant influence on ceiling height
  - Ceiling height may impact delivery of an inert gas fire suppression system

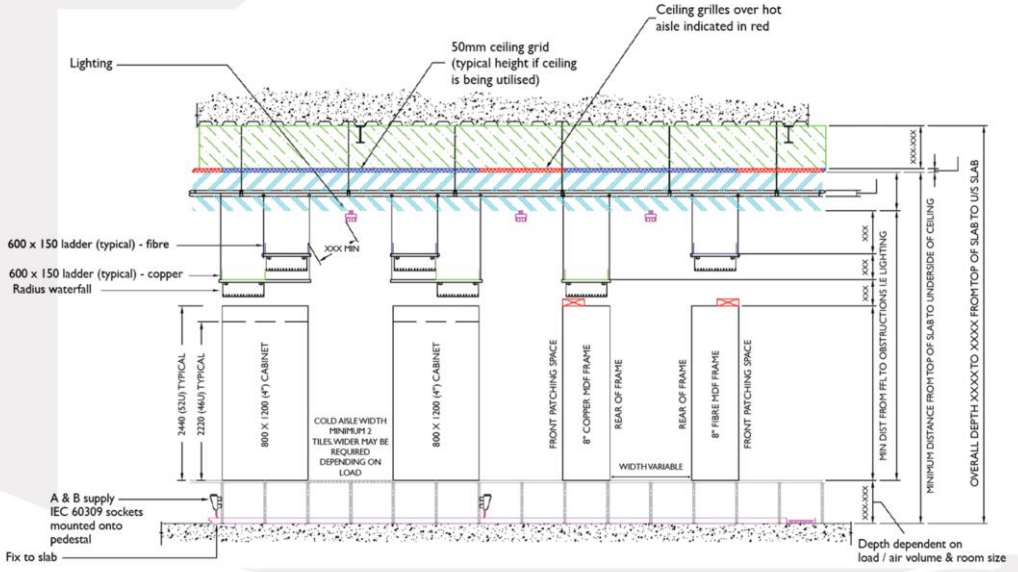
© CNet Training

The building containing the Data Centre must be suitable for the purpose. TIA 942-A provides some very useful best practice recommendations on the building/room structure.

One obvious requirement is being adequately sized to accommodate the data equipment and any ancillary systems.

The minimum requirement to achieve TIA 942-A compliance is 2.6m (8ft 6in). If the Data Centre uses 2.13m (7 ft) racks, then there is not much clearance available. Many Data Centres are built with greater 'slab-to-slab' headroom to facilitate greater clearances. In some cases, a 'slab-to-slab' height of 5m (16ft 5in) is chosen.

Ceiling Heights



© CNet Training

Review

- Are you able to:
  - Review national and international Standards
  - Review the Uptime Institute Tier levels
  - Discuss Data Centre location
  - Discuss Data Centre specifications

© CNet Training

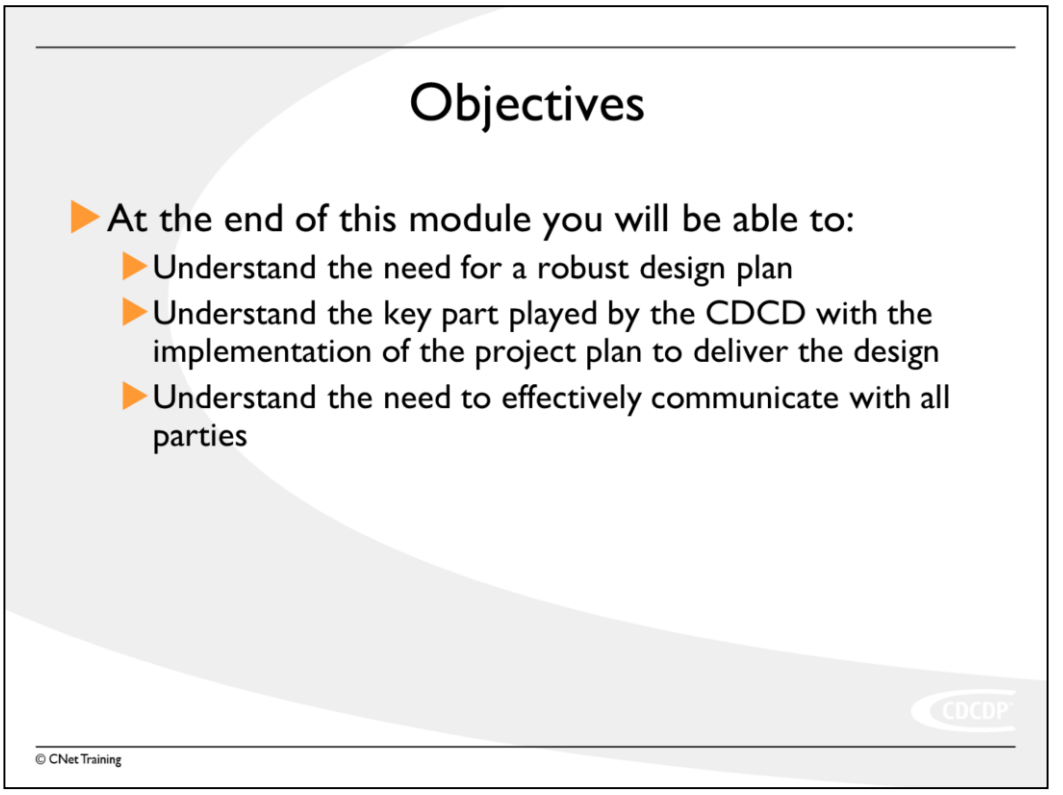
Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

The Design Planning Process

Version 1509



The CDCD is an ambassador to many areas within the company: IT infrastructure, Facilities are merely the tip of the iceberg! As such, you will be called upon to "wear many hats", and thoughtfully interact across numerous disciplines and organisational levels.

Main Design Considerations

- Design decisions will affect the operability of the Data Centre throughout its complete lifecycle
  - Profiles are needed to determine the initial and expected Day One and Day Two capacity requirements for space, connectivity, containment, power load, distribution and cooling
  - Network configuration should be modelled, to account for diversity, redundancy, routing, etc.
  - A planning regime is required that should be followed throughout the design and facility lifecycle
  - Ongoing reviews should continue across the life of the Data Centre

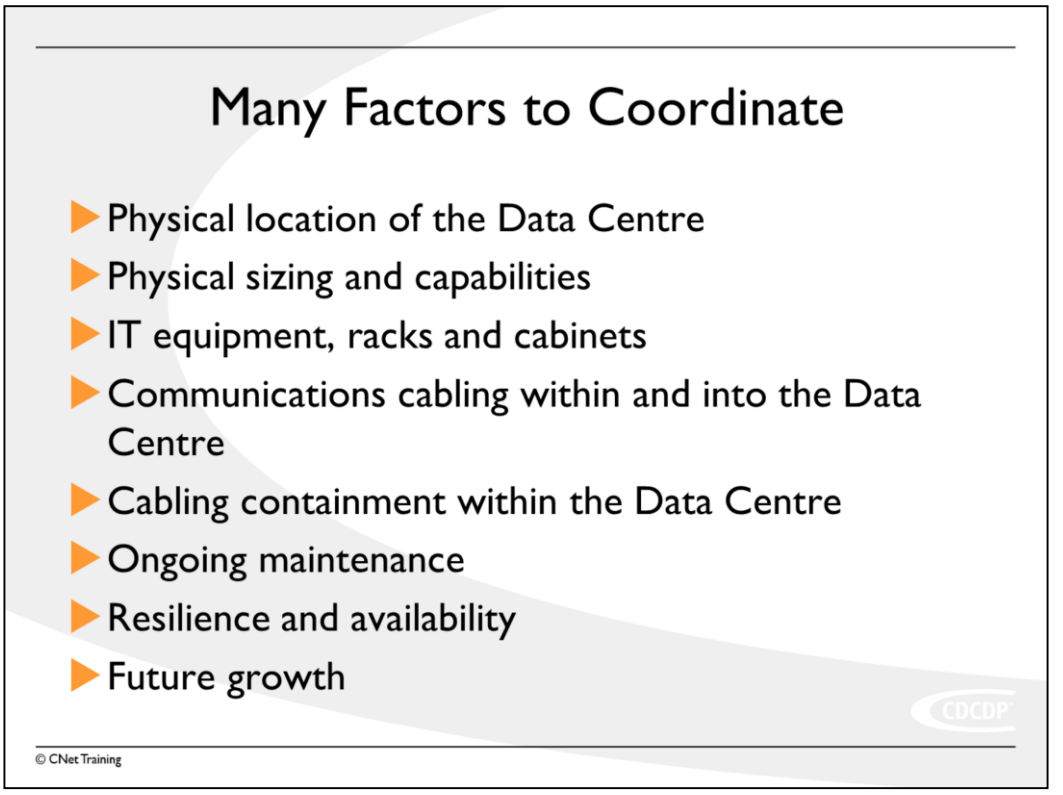
© CNet Training

At the initial planning stages, key decisions are made that affect the operability and maintainability of the Data Centre. Once plans have been implemented and are operational, it is extremely difficult to rectify major problems that can (and often do) lead to inefficient and costly operations and maintenance.

When planning a Data Centre, it is important to evaluate the overall service capacity of the site, with respect to the proposed service provision.

This may be a phased build. Therefore, profiles for each phase should be created, incorporating key decisions with respect to the demarcation of space, power, cooling capacity and connectivity requirements for each phase.

It is vital at the outset to make the correct decisions relating to the configuration and planning regimen for the Data Centre, as this should become the operational model for its lifetime.



The design of a Data Centre is a multi-disciplinary exercise, and the CDCD must be aware of the complex relationships between the various elements: Sizing and capability statements are crucial. IT personnel cannot accurately say what they require when the building is being designed, as they are at least two years away from fitting equipment.

Appreciation should be given to cabinet dimensions and projected weight; failing to properly assess these factors can lead to cable architecture and cabinet layouts which cannot readily accommodate changes in equipment connectivity.

Cable routing and containment depends on (and influences) other design decisions such as airflow management. The determination to route cabling under the floor or overhead can impact the lifetime operation of the Data Centre.

Coordination of Trades

- During the design phase, the CDCD may have to liaise with or work alongside a number of trades, covering aspects such as:
  - IT equipment and systems
  - Electrical systems to and within the Data Centre
  - Ventilation, airflow and HVAC
  - Fire minimisation, detection, alarm and suppression
  - Control, monitoring and reporting
  - Security, access and CCTV
  - Building management systems (BMS)

© CNet Training

All of these allied trades will play some part in setting the design criteria. Each has its own culture and language for its discipline; they often don't understand how to properly integrate with other trades.

Communication is therefore essential to ensure all parties and respective trades are aware of the bigger picture and work together to achieve the end goal.

Multi-Disciplinary Team Approach

- A Data Centre design and subsequent implementation project will incorporate many different stakeholders and trades, all with different tasks and reporting channels
- It is essential a multi-disciplinary team is established to successfully control and coordinate these different elements
- It is also essential the dependencies between different technology layers are fully understood and implemented in the correct sequence, to prevent unnecessary change requests and delays

© CNet Training

A multi-disciplinary team approach enables stakeholders and different trades to:

- Show a commitment to both the project and the team
- Understand project goals and targets
- Collaborate to create innovative solutions to project issues
- Define roles, responsibilities, accountability and expectations
- Review productivity and effectiveness
- Improve communications
- Feel a sense of purpose and camaraderie
- Enable better conflict resolution, reducing difficulties and obstacles
- Increase job satisfaction

The CDCD will have a key part to play within any multi-disciplinary team.

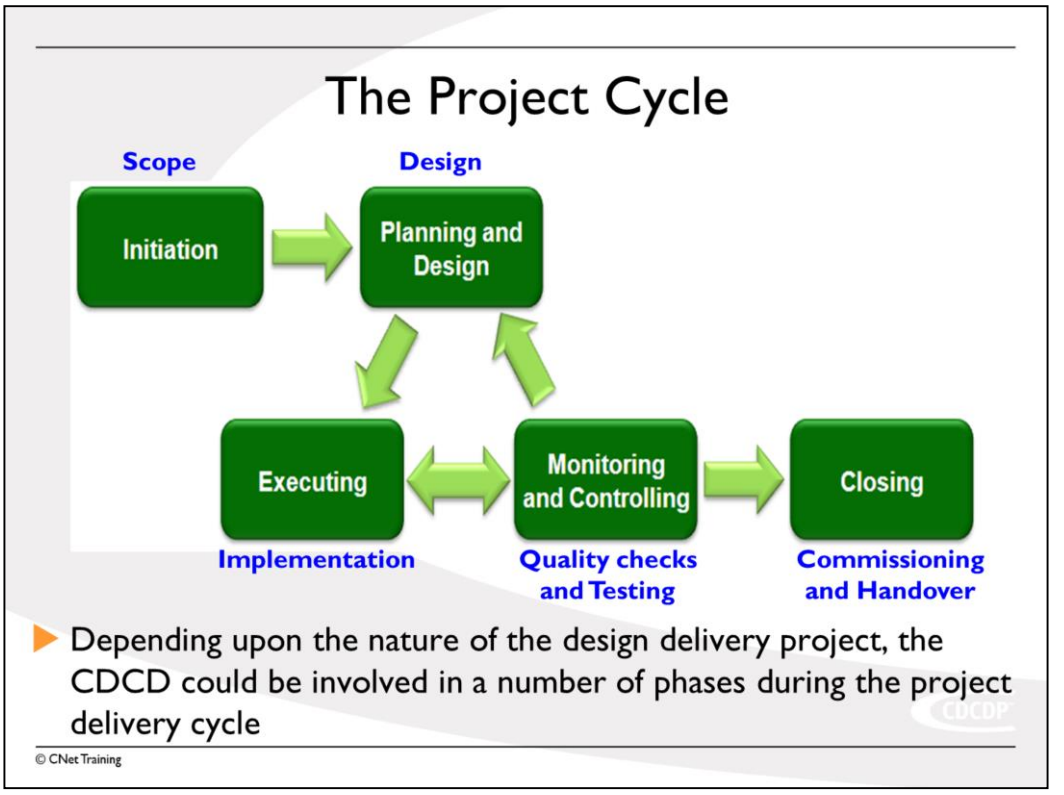
Project Plan Development

- The successful design, commissioning and final handover depends on a robust plan
- Plan so that commissioning and acceptance starts with the design phase, and takes place at every stage throughout the design and build – not just at the end!
- Plan so errors are rectifiable throughout the project lifecycle
- Plan so variations are agreed upon, and their impacts on design are evaluated and considered throughout the project

CDCDP

© CNet Training

A robust plan is critical to the delivery of any Data Centre design project. The plan should ensure acceptance and commissioning tests and record production are built in from the design stage onwards. It is not acceptable to leave them to chance, or to the end. As previously mentioned, the CDCD may be involved in a number of project cycle phases, especially when factors impact upon the agreed design.



- **Initiating process.** Every project requires a start. Stakeholder influences, risk and uncertainty are greatest at the start of the project. These factors decrease over the life of the planning process and project itself. Stakeholders are persons or organisations actively involved in the project, whose interests may be positively or negatively affected by the performance or completion of the project.

  A project charter provides the project manager with the authority to apply resources to project activities. The trigger is a needs analysis, business case, or a response to a customer demand or Request for Quote (RFQ). It includes the project purpose, objectives, requirements, description, risk, milestones and budget.
- **Planning process.** This develops the project plan. The plan will need to be revisited to 'steer the ship' and is known as rolling wave planning: Collecting requirements, scope definition, Work Breakdown Structure (WBS), defining & sequencing activities, estimating resources, durations and costs; development of a schedule and budget, planning for quality, HR, risk communications and procurement.
- **Executing process.** A large portion of the budget is spent on the executing process: Managing execution and quality assurance, acquiring and developing a team, managing the team, distributing information, overseeing stakeholder expectations and procurement.
- **Monitoring and controlling process.** Monitoring and control of work, integration of change control, validation and oversight of scope, schedule and cost. Quality control and performance reporting; monitoring / managing risk and procurement administration.
- **Closing process.** Verifies the processes are in fact complete - Conclude the project or phase, close procurement, document lessons learned and obtain customer acceptance.

Communication

- Communication skills are a key requirement of the design process. The CDCD should provide regular communication and feedback to relevant stakeholders and supporting trades - it should be:
  - Consistent
  - Verbal and written
  - Presented using appropriate media
  - Timely and meaningful
  - Incorporate relevant stakeholders
  - Clear and unambiguous
  - Have an appropriate response level

© CNet Training

The CDCD has the opportunity to be an excellent service provider and focal point: It is easy to overlook the importance of cultivating a great customer service ethic amidst learning these numerous technical specialties.

Design Team Coordination

- Design projects should, by their nature, be directed towards achieving a definite end result
- Individuals at all levels within the design team should be able to stimulate action, progress and change through their personal and professional behaviours
- Where does the CDCD stand in regard to control and co-ordination of the design team?

Source: BS6079-1

© CNet Training

Aspects that a CDCD should be able to undertake:

- Demonstrating initiative, being objective and result-focused
- Displaying strong influencing and persuasive skills
- Delegating effectively
- Managing the effectiveness of the design team as a whole, and the contribution of its individual members
- Being competent at running effective design meetings and communicating

Review

- Can you?
  - Understand the need for a robust design plan
  - Understand the key part played by the CDCD with the implementation of the project plan to deliver the design
  - Understand the need to effectively communicate with all parties

© CNet Training

Any Questions?

© CNet Training

Case Study – Exercise 1

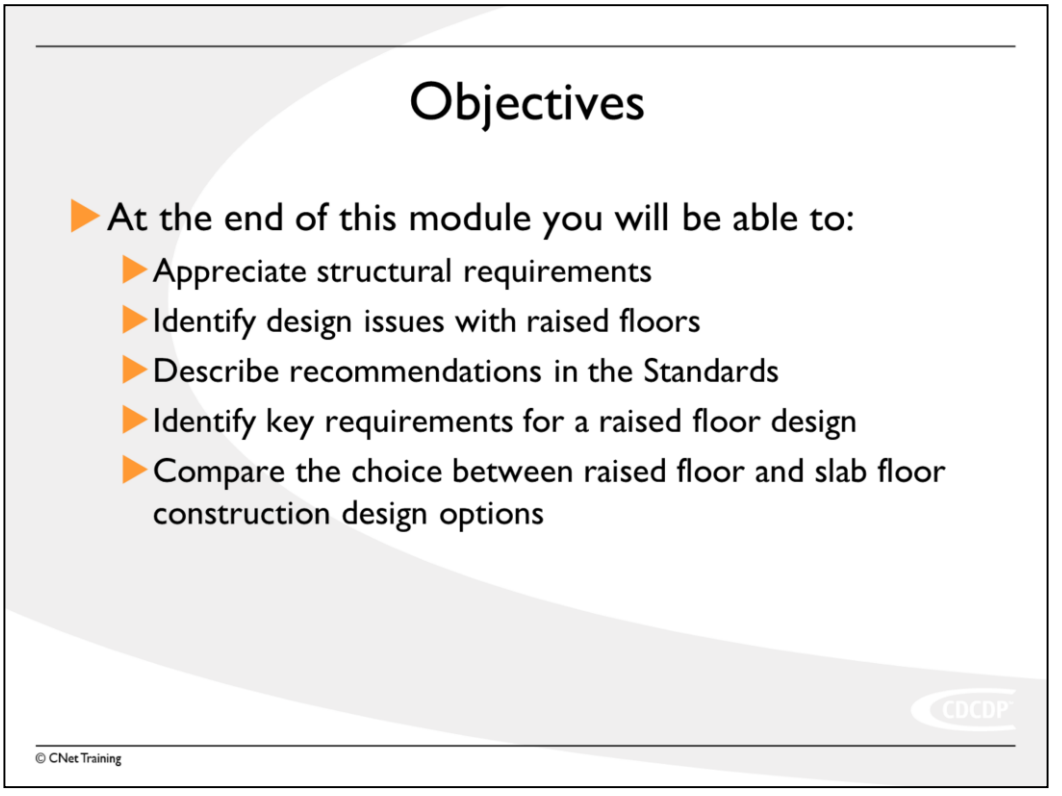
© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

Raised Access Floor

Version 1509

CDCDP



With the increased density and weight of cabinet installations, floor loading capability has become a major concern, with new designs using the slab floor construction approach over the traditional raised floor approach. However, for many Data Centre operators, the raised floor remains popular.

This module will primarily focus on the design requirements of the raised floor application, but will also consider the applicable aspects of slab floor construction design.

Structural Considerations

- What is the structural capability of the floor?
- What is the projected load bearing demand upon the floor?
- What are the projected concentrated and distributed weight loads?
- Are there any floor hanging capacity issues?
- What key personnel need to be involved in the floor design process?

© CNet Training

When considering the options of a raised access floor or slab floor construction design, there are some key personnel you need to consult. In order of priority:

- Structural engineer – To calculate the load bearing capability of the slab floor
- Facility and IT managers – To determine the projected weight of both plant and IT equipment (against the full design forecast)
- Floor vendor – To ascertain the construction and quality of raised access floor required to support the project weight load

Concrete flooring foundations are typically sturdy and long-lasting, due to the fact cement is a sturdy, strong material. But like any type of foundation, they can still be damaged by a variety of factors, including: Moisture damage, earthquakes, poor installation, poor or improper preparation, inferior materials, unlevelled flooring

Raised Access Floor Standards

USA

- TIA 569B
- TIA 942-A

Europe

- Legacy national Standards (pre-2001):
  - VDI 2054 was the industry Standard in Germany
  - MOB PF2 PS was the *de facto* industry Standard in the UK
- This was until the arrival of BS EN 12825
- Local building and fire regulations

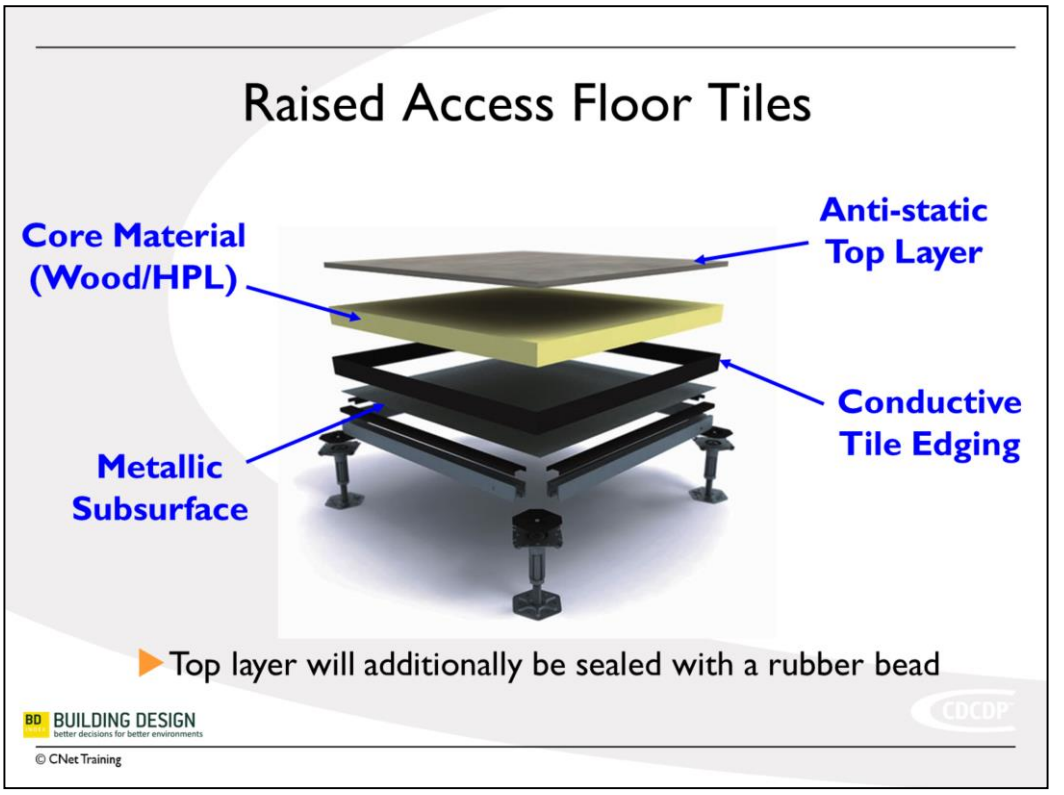
© CNet Training

- In the USA, TIA 569B is the reference Standard.
- BS EN 12825 is the European Standard which supersedes earlier legacy national Standards.

The CDCD should also be aware of local building and fire regulations, which maybe aligned to specific codes or Standards. These include:

- UL 94 – Flammability testing
- EN 13501/1 – Fire test to building material
- The USA has a number of codes and Standards related to flammability of building material, such as NFPA 287 and 701

In all cases, the CDCD should consult the local Authority Having Jurisdiction (AHJ) to confirm relevant codes or regulations.

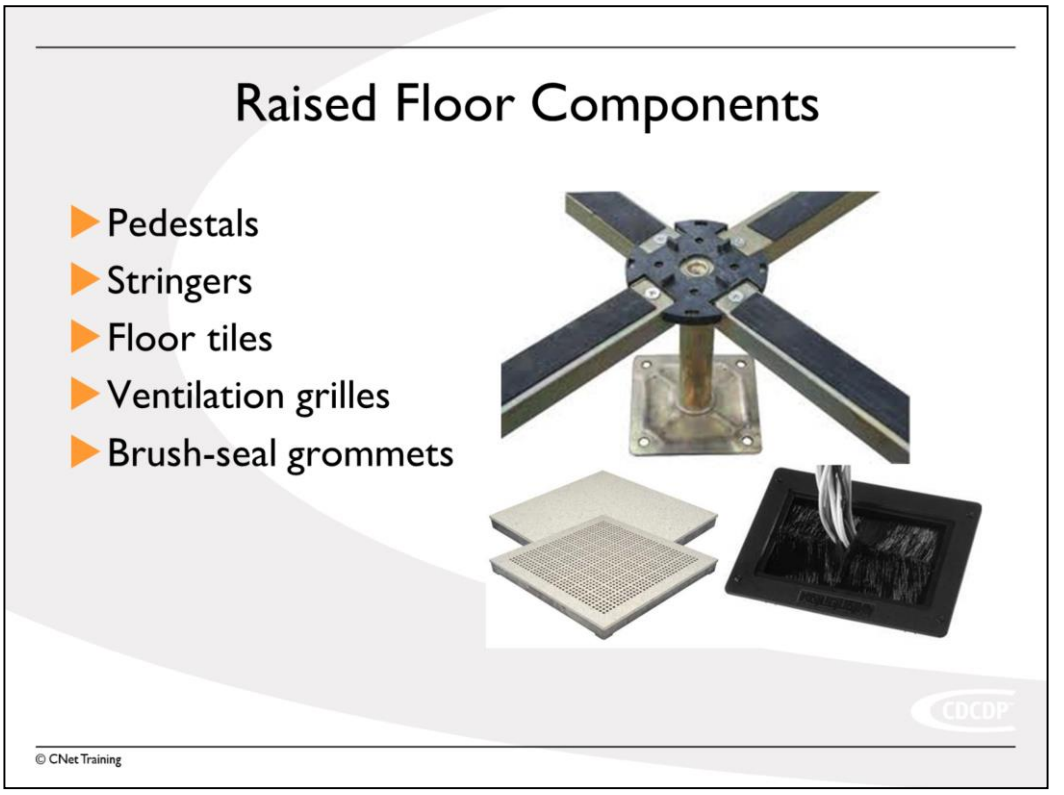


Raised floors are positioned on pedestals, which may be glued or bolted to the floor. The slide shows the construction of a floor tile with a wood or high-pressure laminate (HPL) body. Within some older Data Centres, the tiles are made from aerated concrete or ceramic fill; these do not generally fail in a graceful manner and often snap!

The CDCD should be aware of the differences between metric and imperial measurements. For example:

- European floor tiles are 600mm x 600mm
- US floor tiles are 24in x 24in (610mm x 610mm)
- Seismic zones may have 500mm x 500mm tiles (19.7in x 19.7in)

The CDCD should also be aware that different manufacturers' products are not always interchangeable.



- **Pedestals** may be adhesively or mechanically fixed to the slab, with locating lugs on the head to ensure correct panel seating; they provide the option of screw-fixing for additional rigidity.
- **Stringers** provide additional lateral stability. Where floor heights exceed 600mm, stringers may be attached to the pedestals. Stringers will improve integrity and rigidity but will not affect load-bearing performance. They should be bolted to the pedestal.
- **Ventilation grilles** for underfloor HVAC systems are available, including perforated or bar-grilled formats.
- **Brush-seal grommets** are designed to fit into raised flooring panels in pressurised plenum environments, to maintain pressure where floor penetrations are required.

Loading - TIA 942-A

- Floor loading capacity in the computer room shall be sufficient to bear both the distributed and concentrated load of the installed equipment with associated cabling and media
- The minimum distributed floor loading capacity shall be 7.2 kPA (150 lb/ft^2)
- The recommended distributed floor loading capacity is 12 kPA (250 lb/ft^2)
  - Some Data Centres specify 60 kPA (1250 lb/ft^2) or more

CDCDP

© CNet Training

The floor must be able to support the weight of the equipment for both concentrated and distributed loads.

Can you picture what 12kPA really means?

- 1 kPA = 0.01 bar
- Therefore, 12kPA = 0.12 bar
- 1 bar is equivalent to a column of water, approximately 10m high.
- Therefore, 0.12 bar is equivalent to a column of water, approximately 1.2m (4ft) high.

Just to highlight to the CDCD - Standards are really a minimum requirement. Some Data Centres specify 60kPA (1250 lb/ft^2) or more, which is well above the Standard. More specific load dimensions can be assessed within TIA 569B and BS EN 12825 respectively.

Loading - TIA 569B

	Impact Load Drop weight equals 305mm (12in) on 645mm² (1in²) local surface deformation 1.5mm (0.06in)		Concentrated Load 645mm² (1in²) Maximum deflection 2mm (0.08in) from anywhere on the panel		Ultimate Load 645mm² (1in²) Accepts load without failure		Uniform Load Maximum deflection 1mm (0.04in) from bottom anywhere on the panel	
	kg	lb	kN	lbf	kN	lbf	kg/m²	Lb/ft²
General Office								
Medium Duty	45	100	272	2.7	816	8.0	732	150
Heavy Duty	57	125	454	4.4	1361	13.3	1221	250
Equipment Room								
Light Duty	45	100	272	2.7	816	8.0	732	150
Medium Duty	57	125	454	4.4	1361	13.3	1221	250
Heavy Duty	68	150	567	5.6	1701	16.7	1465	300
Information Process Centre								
Light Duty	57	125	454	4.4	1361	13.3	1221	250
Meduim Duty	68	150	567	5.6	1701	16.7	1465	300
Heavy Duty	79	175	680	6.7	2041	20.0	1709	350

TIA 942 recommended

TIA 942 minimum

© CNet Training

TIA 569B refers to raised floor systems, which are classified in terms of impact load, concentrated load, uniform load and ultimate load in terms of deflection and dimensional tolerances.

Where does the Data Centre fit into this table?

- TIA 942 Minimum 7.2 kPA (732 kg/m² 150 lb/ft²)
- TIA 942 Recommended 12 kPA (1221kg/m² 250 lb/ft²)
- Concentrated load: The access floor panel's capability to handle a point or static load. Use Ceilings and Interior Systems Construction Association (CISCA) testing guidelines for concentrated load
- Uniform load: The load applied over the entire area of the panel in lb per m² or ft²
- Rolling load (or dynamic load): The access floor panel's capability to handle movement of equipment on wheels. Rolling loads are determined by the number of passes, the size and hardness of the wheels. Rolling loads typically have a more damaging effect on a panel than a static load
- Impact load: Defined by the weight of the load and the height the object is dropped
- Ultimate load: The load at which the panel structurally fails, and is sometimes expressed as a multiple of concentrated load

Loading - BS EN 12825

Application Area	BE EN 12825 Classification			Finished Floor Height		
	Light Use	Standard Use	Heavy Use	Cable Management	Cable Management & HVAC	Floor Finishes
General Office	1/A/3/2	3/A/3/2	5/A/3/2	50-150mm	300-450mm	Carpet Tiles
	1.33kN Working Load	2.67kN Working Load	3.3kN Working Load			
Service Corridors	1/A/3/2	3/A/3/2	5/A/3/2	50-150mm	300-450mm	Carpet Tiles
	1.33kN Working Load	2.67kN Working Load	3.3kN Working Load			
Computer Rooms	1/A/3/2	4/A/3/2	6/A/3/2	n/a	300-600mm	Vinyl / HPL
	1.33kN Working Load	3kN Working Load	4kN Working Load			
Internet						
Data Centre	4/A/3/2	6/A/3/2	6/A/3/2	n/a	300-600mm	Vinyl / HPL
Data Centre	3kN Working Load	4kN Working Load	4kN Working Load			
Comms Rooms	1/A/3/2	4/A/3/2	6/A/3/2	300-450mm	300-600mm	Vinyl / HPL
	1.33kN Working Load	3kN Working Load	4kN Working Load			

© CNet Training

Floor heights in BS EN 12825 vary depending on application. In a computer room, the height could be from 300mm (12in) to 600mm (24in).

Additional lateral strength may be facilitated by stringers. These become more important as the floor height increases.

BS EN 12825 refers to ultimate loading measured on a 25x25mm area in the centre of the tile, so it is not easy to directly compare with TIA. BS EN 12825 has established six ultimate load classes:

- Class 1 ≥4 kiloNewtons (~225lb)
- Class 2 ≥6 kN
- Class 3 ≥8 kN
- Class 4 ≥9 kN
- Class 5 ≥10 kN
- Class 6 ≥12 kN

Legacy Raised Floor Standard

Grade	Concentrated Load over 25mm sq	Concentrated Load over 300mm sq	Uniformly distributed Load
LIGHT	1.50 kN	2.70 kN	6.7 kN/m^2
MEDIUM	3.00 kN	4.5 kN	8.0 kN/m^2
HEAVY	4.50 kN	N/A	12.0 kN m^2
EXTRA HEAVY	4.50 kN	N/A	12.0 kN m^2
	In addition, this grade is required to sustain a total load of 11 kN applied equally on four points, each point 25mm sq on a 200 mm x 200 mm square configuration anywhere on the system.		

- Data Centre raised floors pre–2000 may have been installed to the Method of Building Performance Specification 'Platform Floors (Raised Access Floors)' MOB PF2 PS specification
- MOB PF2 PS details three primary floor grades

© CNet Training

When undertaking retrofit or upgrade design work, the CDCD must be aware the raised access floor could have originally been installed to MOB PF2 PS Standard specification.

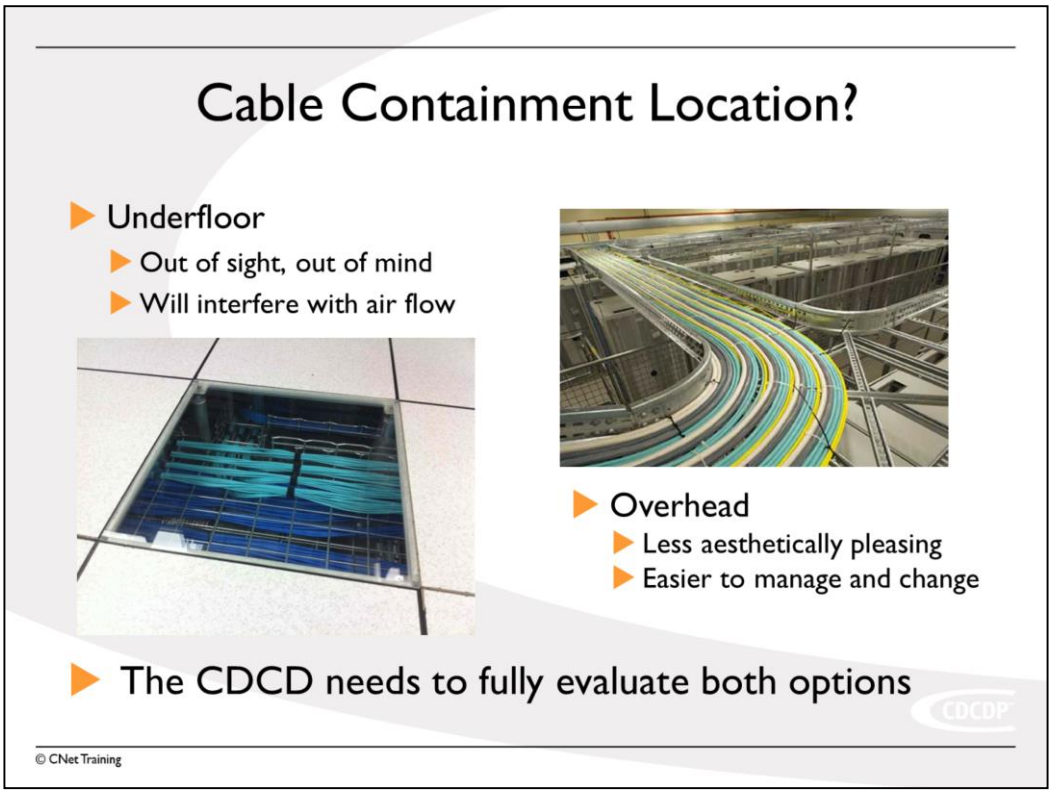
Impact on Ceiling Height

- The height of the floor must be worked out in conjunction with the ceiling height
  - The minimum height in the computer room shall be 2.6m (8ft 6in) from the finished floor to any obstruction, such as sprinklers, lighting fixtures or cameras
  - A minimum of 460mm (1ft 6in) clearance shall be maintained from water sprinkler heads
    - Sprinklers are classed as life safety systems and have some code or regulatory requirements

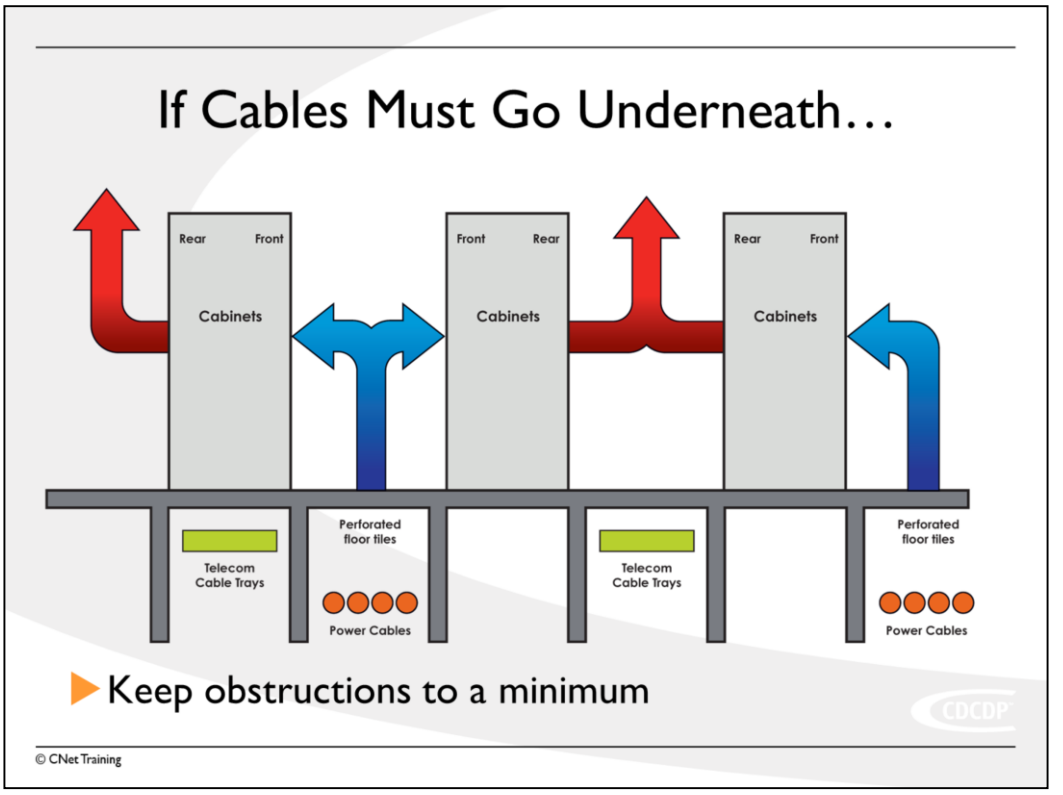
Source: TIA 942-A

© CNet Training

There are architectural constraints on how high the floor can be. Remember that raised floors may affect the minimum height of the ceiling - this is one of the reasons slab floor construction designs are becoming more appealing.

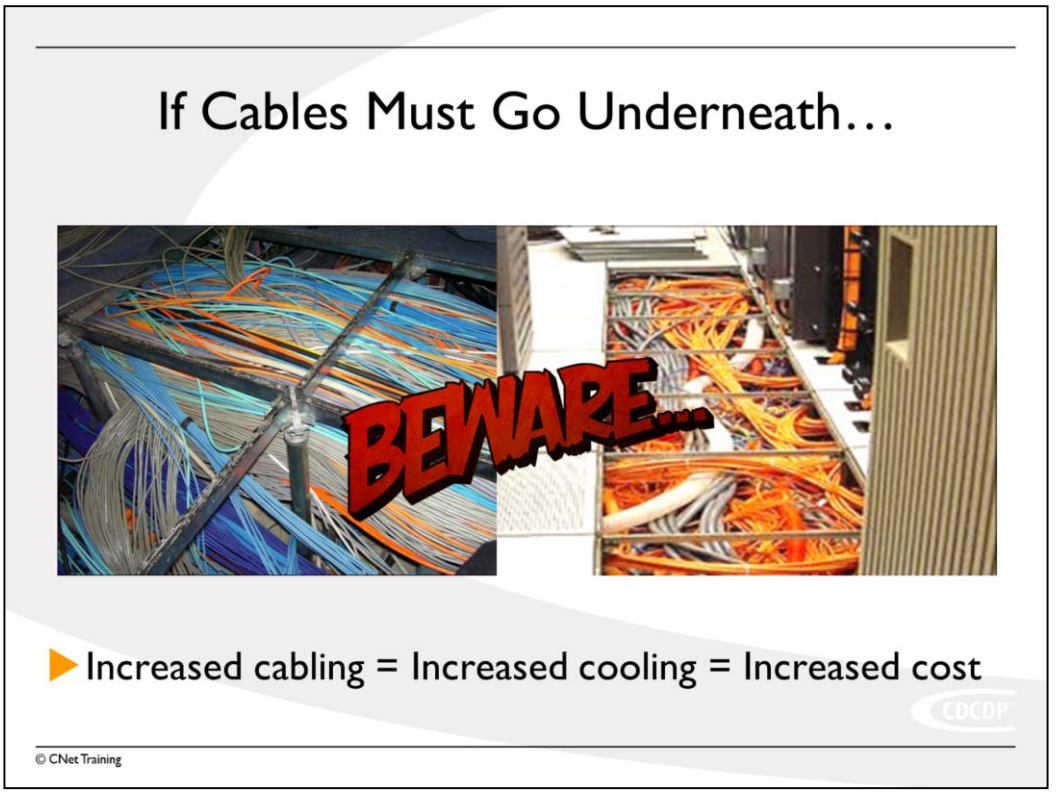


One of the fundamental factors affecting the space required under the floor is the choice of cable routing. If cables are routed under the floor, it increases the space required; the more cable, the more space - and often unforeseen impacts upon cooling distribution.



Underfloor cables must not impede the flow of cooling air, but they regularly do. A rule of thumb is to run power cables in the cold aisle, as they tend to be fewer. Data tray work can ideally be run in the hot aisle where there are no perforated tiles or, in a pinch, partially under the cabinets (this makes access difficult).

The CDCD should make a decision based on the requirements of the room and the space available.



The floor is not just there to stand things on. It is an integral part of the Data Centre. If floor integrity is compromised (and it often is), it seriously affects the cooling system and can greatly increase the running cost of the Data Centre. This kind of cabling negates the plenum zone effectiveness for air distribution. Underfloor cable distribution needs to be well planned, with disciplined installation procedures.

There have been numerous industry surveys detailing significant impacts upon the quality and delivery capability of cooling systems:

- "Poor airflow management takes 50% or more of the CRAC capacity" (Source: Pacific Gas and Electricity)
- "60% of the cooled air in a typical Data Centre does not flow to where it is needed" (Source: Uptime Institute)
- "70% of cooling air is wasted and bypasses back to return system" (Source: Mazzetti Associates)

If Cables Must Go Overhead…

- Overhead clearances and weight impacts need to be properly assessed

© CNet Training

This is especially relevant when considering the potential impact of raised floor hanging loads within a multi-floored environment.

Colour and Anti-Static Properties

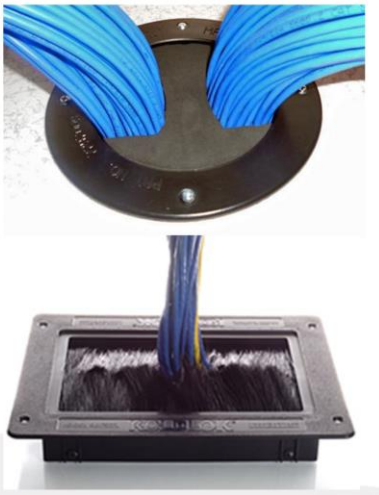
- The raised floor tiles and/or finished floor surface should be light in colour to enhance room lighting
- Floors shall have anti-static properties as per IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity test
  - Carpets are taboo!
- Dirt and scuffing reduces anti-static properties
  - Keep it clean
  - Keep it maintained

© CNet Training

The finish of the floor can affect the overall performance of the Data Centre. This equally applies to raised floor tiles. Keeping the floor's surface clean is especially important for maintaining its conductive properties. The floor itself is a mechanical system and should regularly be maintained the same as any other piece of equipment within the Data Centre.

Sealing the Floor - Efficiency

- Chilled conditioned air will be able to escape through poorly finished floor tiles, wall seals and service penetrations, leading to:
  - More electricity consumed to replace lost conditioned air
  - An inability to deliver the volume of chilled air required at the floor vents
  - A variation in air pressure across the floor, leading to an inability to deliver chilled air at the air vents
  - Increased bypass opportunity



© CNet Training

The plenum zone created must be sealed, free of dust, with no unsealed cable or pipework entrances. A poorly sealed floor can lead to additional unnecessary cost.

Sealing the Floor - Safety

- Unsealed service penetrations are a fire risk
- Gaseous fire suppression systems depend upon a sealed area to work properly
- Perimeter seals need to be installed
- Pressure testing is also highly recommended

© CNet Training

Running costs are not the only reason for sealing. Unsealed service penetrations, such as cables and pipes into the plenum area are a fire risk, and will allow the spread of fire and smoke into or out of the computer room (Building regulations, part B).

Gaseous fire suppression systems rely on lowering the level of oxygen available to fires as well as a sealed area to work (to prevent oxygen from resupplying the fire). BS ISO 14520 P1: Gaseous fire-extinguishing systems - physical properties and system design.

A pressure test should be conducted every 12 months.

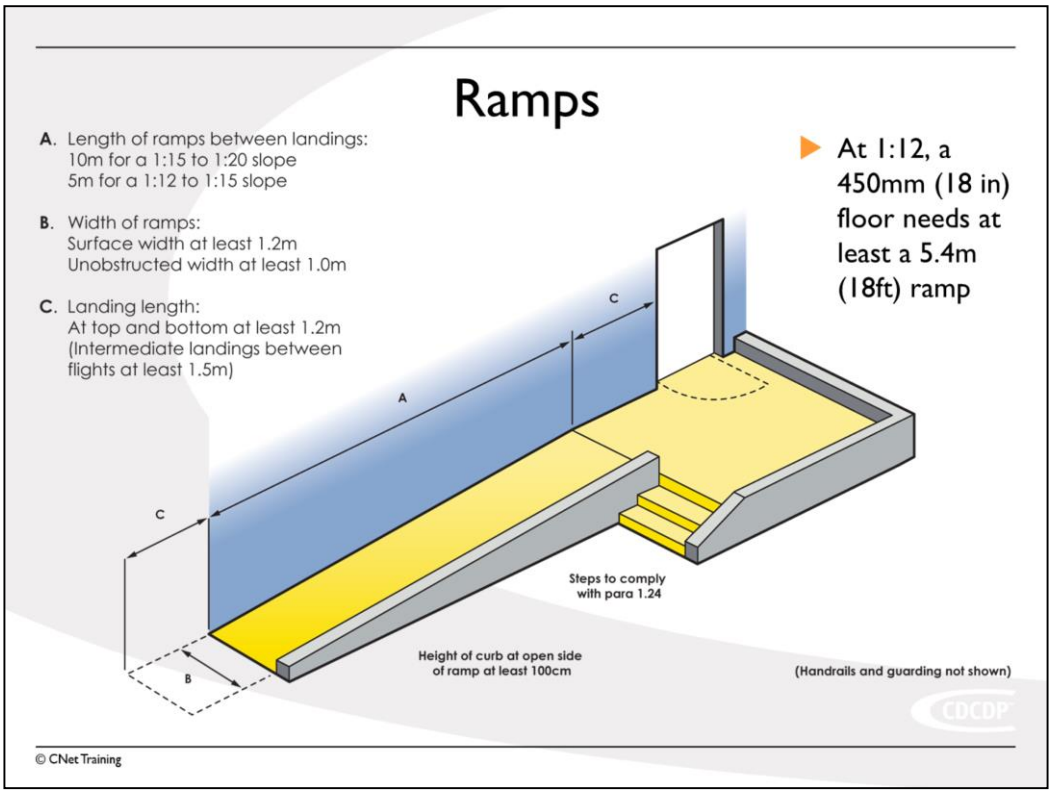
Ramps

- Ramps and steps should be constructed to approved details to achieve performance requirements specified for the associated raised access floor
- UK
  - Ramps: The Building Regulations 2000
- USA
  - Building codes
  - ADA regulations

© CNet Training

The requirements for a raised floor must be carried through into access ramps, etc. even though these are generally outside of the computer room, but not always as illustrated by the above picture.

Note: United States has specified guidelines within the Americans with Disabilities Act (ADA), but the CDCD must also be aware of local building regulations. Always consult with the local Authority Having Jurisdiction (AHJ).



Ramps have a gradient of between 1:12 and 1:20.

They can be quite long, and the CDCD must take this into consideration.

Beware - Zinc Whiskers

- Zinc whiskers grow on metal stringers, or off the bottom and sides of floor tiles with a zinc electroplated-passivation coating on the sheet-metal pan
- Specify hot-dipped galvanised (HDG) or electroplated zinc

© CNet Training

Zinc whiskers are tiny conductive filaments of zinc typically less than a few millimetres (mm) long and only a thousandths of a millimeter in diameter. They grow from metal surfaces (e.g., steel) that have been electroplated (galvanised) with zinc for protection.

Sources of zinc whiskers include the underside of floor tiles, floor pedestals and support rails, as well as equipment racks and hardware such as bolts, nuts and washers.

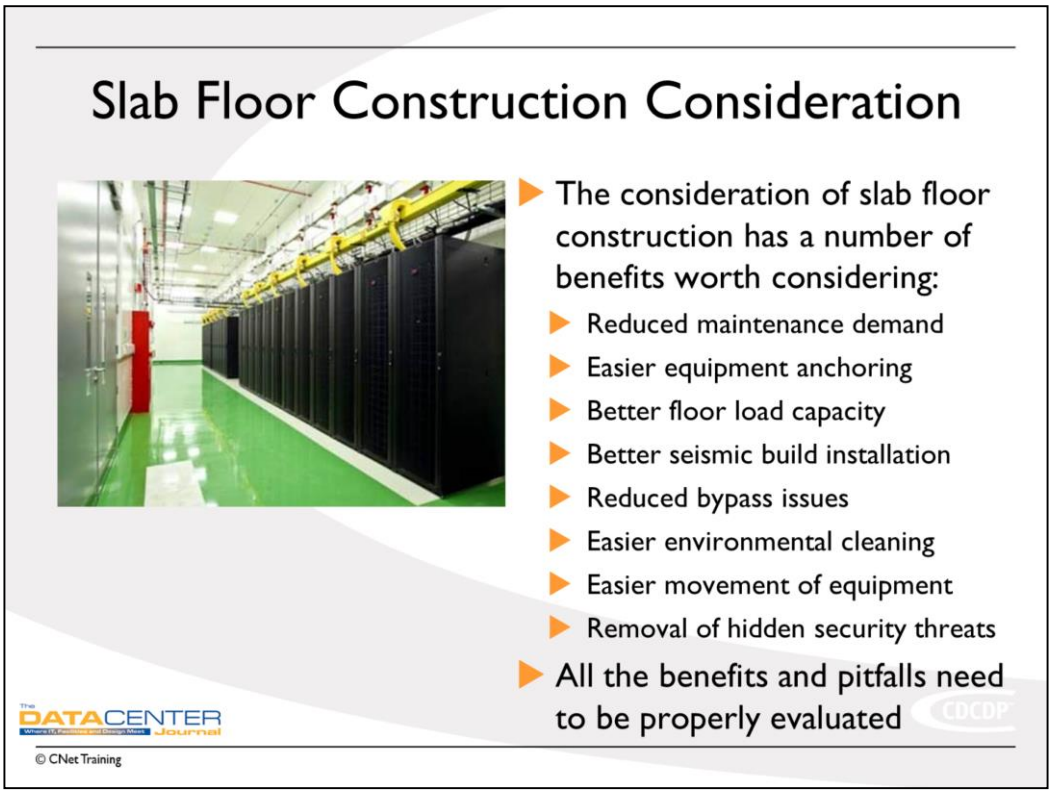
Summary of Raised Floor Design Issues

- Load bearing capacity
- Height
- Finish / décor
- Plan access ramps
- Seal the system for air conditioning efficiency and fire spread reduction
- Earth bond all metalwork
- Good and suitable finish to original floor

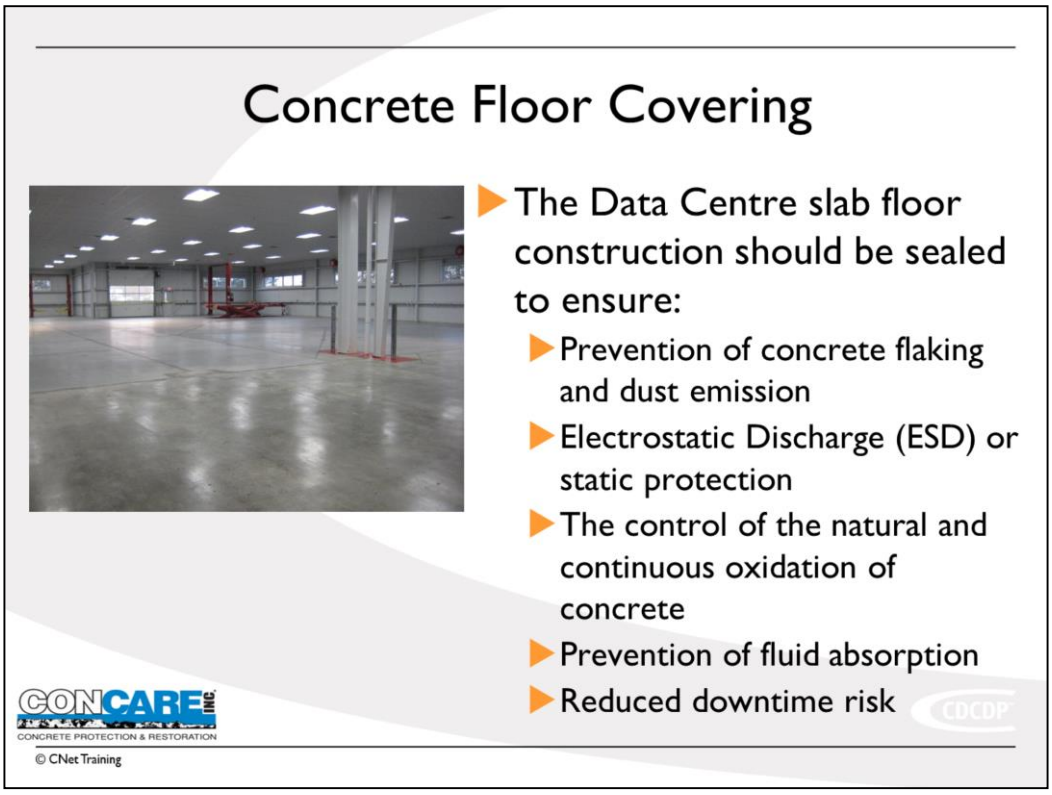
© CNet Training

It has been common practice to use a raised floor, although new solid floor designs are becoming more common.

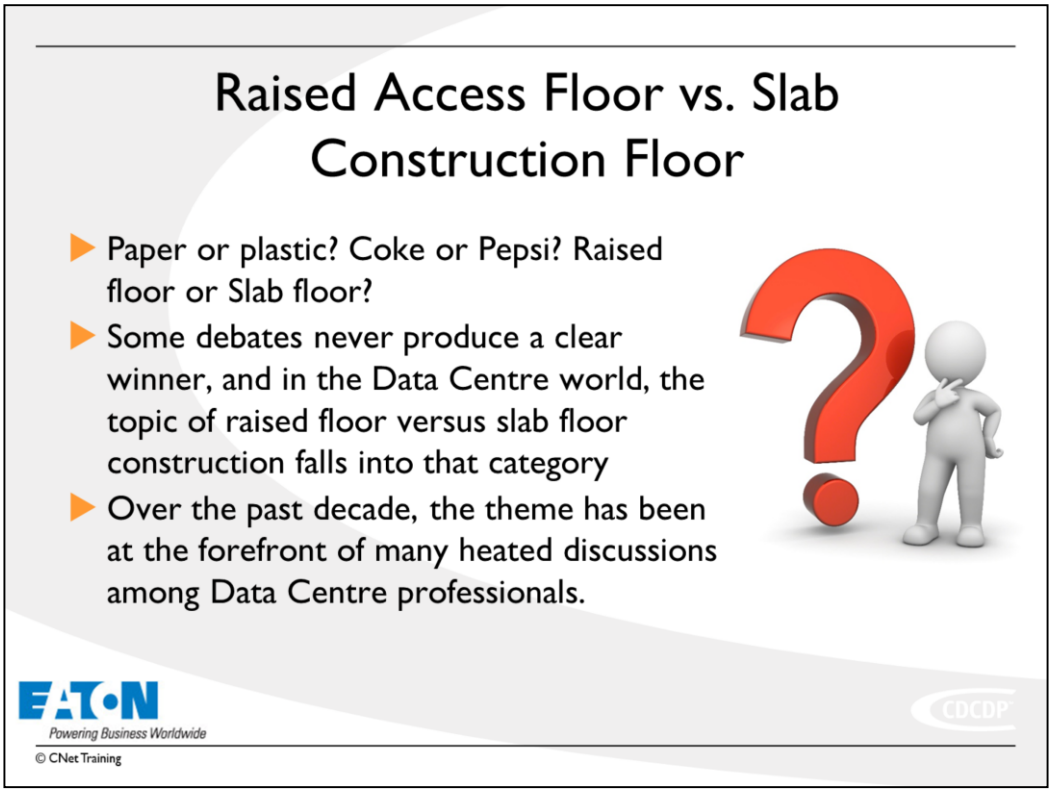
If a raised floor is to be used, there are many considerations the CDCD must be aware of and fully evaluate.



Even though the vast majority of Data Centres still use a raised floor, building on a slab may capture the future. According to the Uptime Institute, only about 48% of companies plan to use raised floors—a distinct drop from the 90% currently using them (2014 Report).



Concrete floor coatings in Data Centres eliminate dust contamination on the concrete floor. Bare or unsealed concrete floors can flake and spall over time, emitting dust particles into the air, becoming hazardous to sensitive equipment as well as the facility. Sealing a concrete floor should be standard practice in a Data Centre environment, especially to control static electricity.



Every Data Centre is unique, and raised floors still make sense for some, so don't expect them to completely disappear from the Data Centre world overnight. But don't be surprised when slabs slowly take over, because they've already started to.

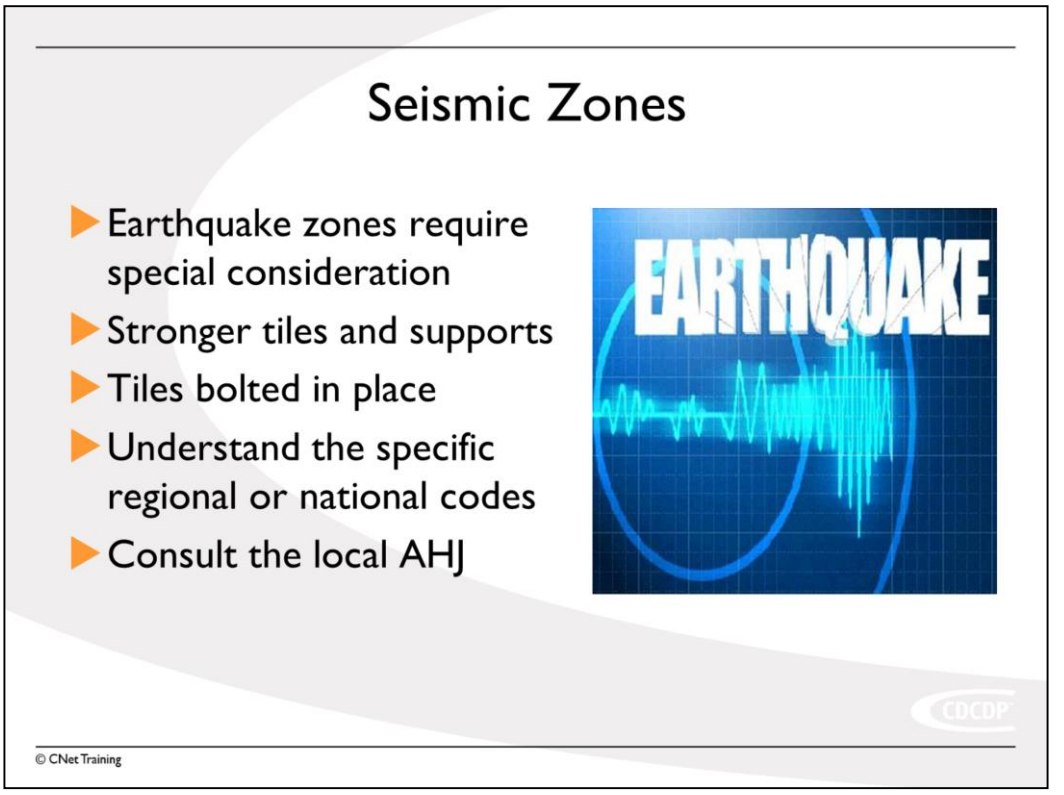
Most construction cost comparisons fail to produce a clear victor as well. The various component costs associated with each approach yield a similar cost per square foot / metre of Data Centre area, according to most studies.

For regions prone to earthquakes, seismic performance is also a consideration, with the slab floor getting the nod. Not only is it a less costly option, but equipment anchoring is easier, and the added lateral bracing and reinforcement associated with a raised floor system are not issues.

Finally, market demand may also play a role in Data Centre design. In some regions of the world, the market simply expects Data Centre facilities to have raised floor. There will remain many factors that sway the decision of raised access floor or slab construction floor. For example:

- The building architecture (purpose-built or aligned to an existing building)
- Flexibility to meet changing demands
- Energy efficiency
- Planning timeframes
- Customer demands

The debate will undoubtedly continue to rumble on for many years, and the CDCD will need to assess the virtue of each option for each potential design project.



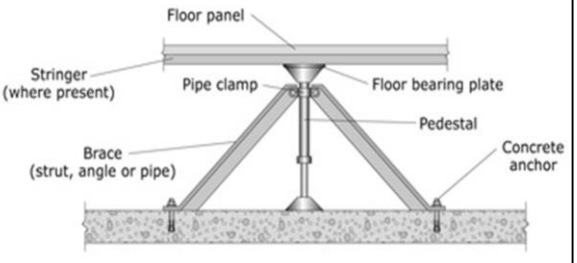
Data Centres in geographic areas prone to seismic activity need to take special consideration when making the decision to install raised floors.

In an earthquake, damage often happens when cabinets resting on casters or pads bounce around on the raised floor, falling into holes left by panels that have shifted. Raised floors designed for seismically active areas have stronger tiles, sturdier support pedestals, and bolts to secure tiles in place. Guidance in the United States is available from:

- The American Society of Civil Engineers Standard 7 (ASCE7) provides a guide for the Selection, Installation, and Use of Raised Computer Floors in seismic zones
- Telecordia Technologies GR-63-Core Network Equipment Building System (NEBS)
- International Building Code (IBC)
- Authority Having Jurisdiction (AHJ) coordinating local regulatory requirements

Braced Access Floor Pedestal

- For new floors in areas of high seismicity
- Meeting the applicable code provisions for 'special access floor'
- Confirm requirements with the local Authority Having Jurisdiction (AHJ)



Braced Access Floor Pedestal
(use for tall floors or where pedestals are not strong enough to resist seismic forces)

FEMA

CDCDP

© CNet Training

FEMA – Federal Emergency Management Agency (US)

Review

- Can you?
  - Appreciate the structural requirements
  - Identify design issues with raised floors
  - Describe the recommendations in the Standards
  - Identify key requirements for a raised floor design
  - Compare the choice between raised floor and a slab floor design options

© CNet Training

Any Questions?

© CNet Training

Case Study – Exercise 2

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

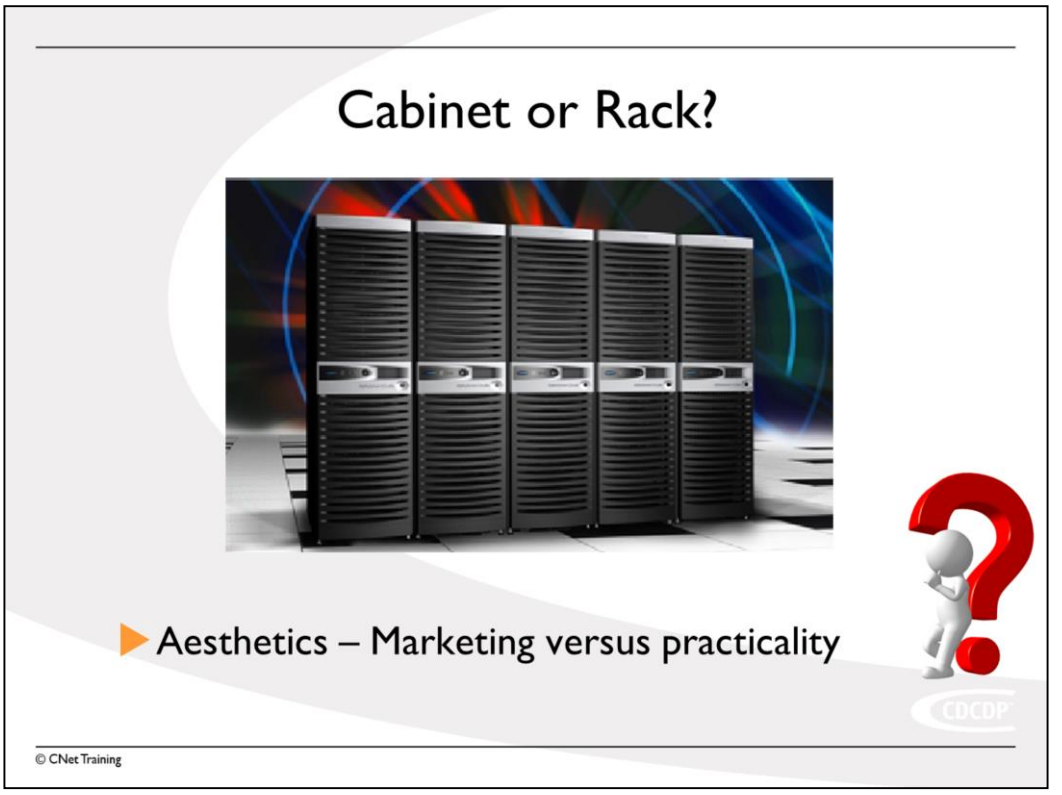
Cabinets

Version 1509

Objectives

- At the end of this module you will be able to:
  - Appreciate cabinet design considerations
  - Describe strategies for effective cabinet layouts

© CNet Training



The terms cabinet, rack and frame tend to be used differently throughout the world. In Europe, an enclosure with doors would normally be called a cabinet, whereas in the USA, it would be called a rack. In the UK, the terms are used interchangeably.

In Europe, an open enclosure would normally be called a rack, whereas it might be called a frame in the USA.

Suites of identical cabinets may look good and would actually be good; however, the reality is a Data Centre has different cabinets from diverse manufacturers, installed at different times during its lifetime. These cabinets can have different characteristics and may not fit together to form uniform rows.

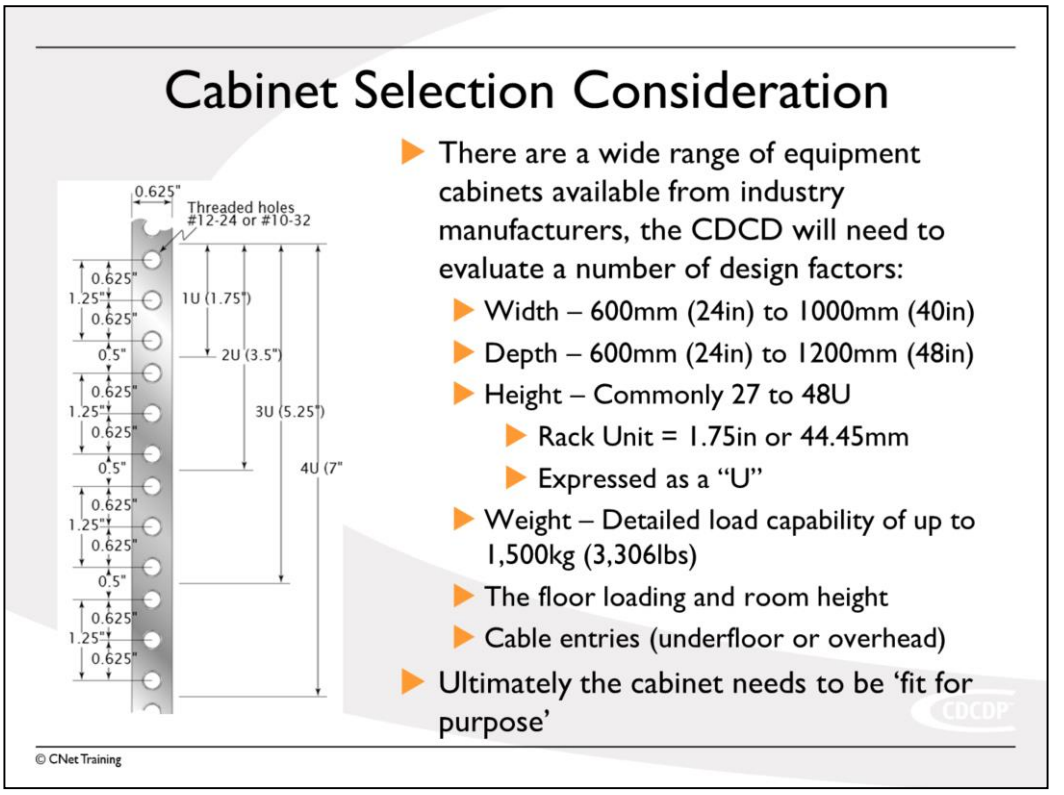
More than just somewhere to mount equipment?

- Aesthetically pleasing?
- Securely hold equipment
- Allow access to hardware and cabling
- Allow adequate ventilation
- Provide secure doors
- Organise power and data cabling
- Provide environmental and security monitoring

© CNet Training

A traditional view of a cabinet had been just somewhere to mount equipment. In a Data Centre environment, this is not the case.

A cabinet is an integral part of the design and must perform a whole raft of functions as shown above. Each function is important.

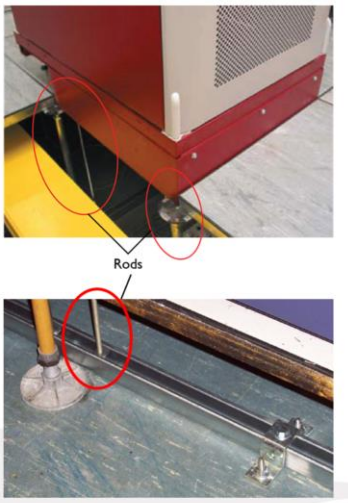


While there is no Standard for the depth of equipment (nor the outer width and depth of the cabinet or rack enclosure itself - incorporating the structure, doors and mounting rails), there is a tendency for 4-post racks to be from 600mm - 800mm (even 1,000mm – 1,200mm) wide. This of course varies by manufacturer, the design of the rack and its purpose; through common constraining factors (such as raised floor tile dimensions), these dimensions have become quite common.

The "U" is the standard unit of measure for designating vertical usable space, or height of racks (metal frames designed to hold hardware devices) and cabinets (enclosures with one or more doors). This unit of measurement refers to the space between shelves on a rack. 1U is equal to 1.75 inches. For example, a rack designated as 20U, has 20 rack spaces for equipment and has 35 (20 x 1.75.) inches of vertical usable space. Rack and cabinet spaces (as well as the equipment which fits into them) are all measured in U.

Security and Safety

- Cabinets supported by the access floor shall be bolted to the cement slab (or a metal channel secured to the slab) by threaded rods that penetrate the floor tiles



Source: TIA 942-A

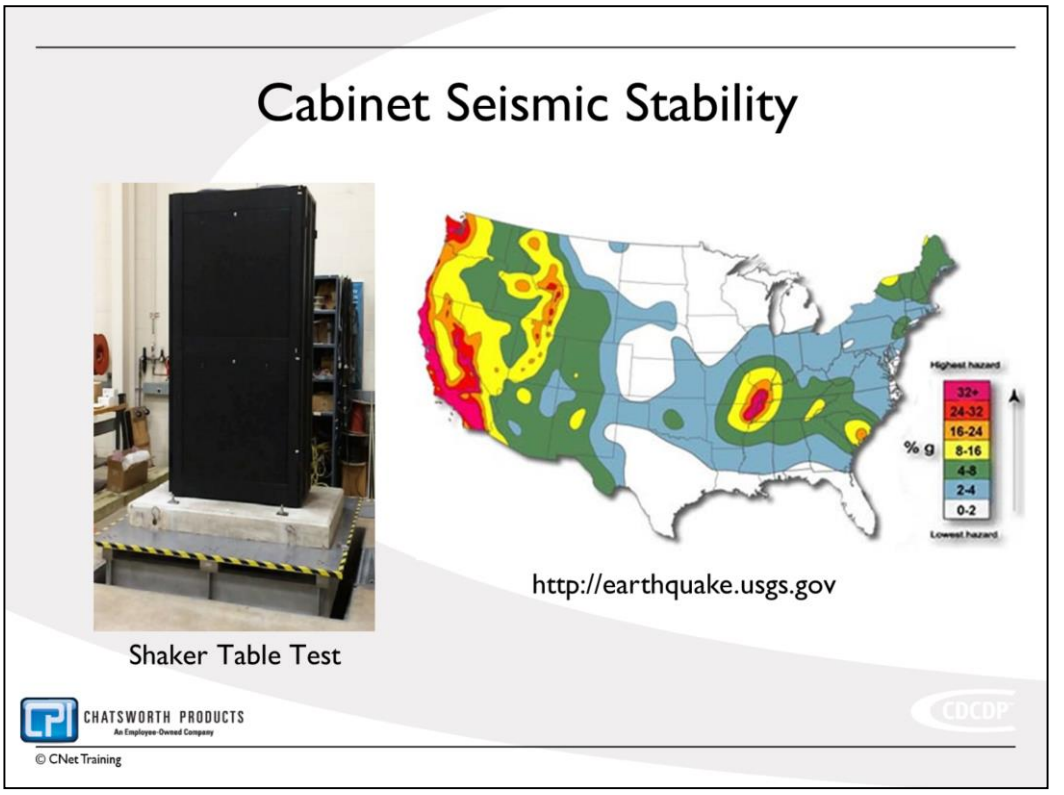
© CNet Training

Cabinets can be heavy - some can now hold 1,500kg (3,306lbs) of equipment. It is important that it not be left to the raised floor to support the full weight: Bolts or pillars that extend the cabinet to the concrete floor are required; these rods can be quite long.

This gets overlooked in many Data Centres, and cabinets are often freestanding or, worse yet, left supported on their castors. The CDCD should ensure security features are built into the design.

Each cabinet must be bolted securely to the floor, or be equipped with extendable anti-tip legs in order to keep it from tipping forward when a server (or other equipment) is extended out of the front of the cabinet.

Always install systems from the bottom up to help stabilise the cabinet. Weight should be installed towards the bottom of the cabinet, but a good tip for the CDCD is to consider leaving 12-15U below the first installed equipment (subject to the type and weight of given equipment).

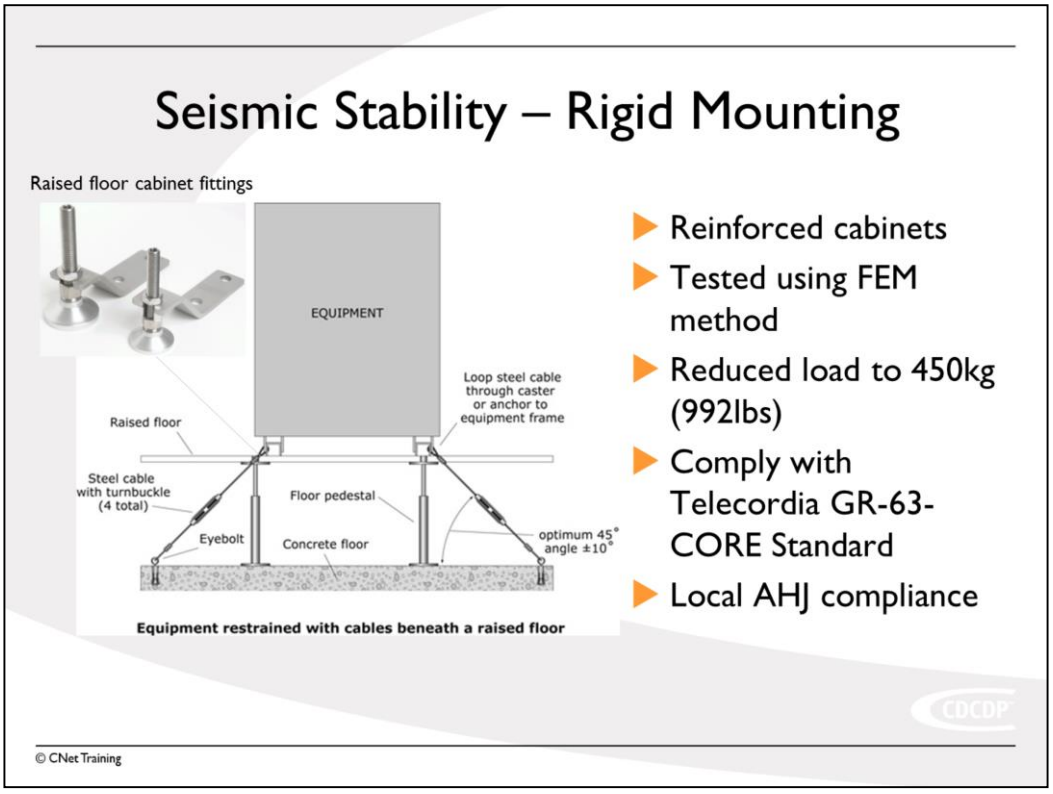


To reduce risk and injury and minimise equipment damage during an earthquake, proper seismic protection is essential and controlled by the local AHJ. This is especially important in telecommunications and equipment rooms, and Data Centres that cannot afford to be offline (not backed up at a secondary location).

Selecting the right infrastructure products for your Data Centre is crucial in order to get the most protection for servers, switches and cables. Specialised equipment and accessories such as racks, cabinets and bracing help minimise excessive motion that may cause undue strain on cable and network connections.

There are many seismic products and solutions available on the market today. To adequately protect equipment, it is important to understand the types of seismic ratings, additional features and benefits needed for proper cable and thermal management.

A shaker table test ensures an enclosure will function properly during seismic events. The shaker table simulates an earthquake (up to 8.3 on the Richter scale) and shakes the enclosure front-back, side-side and up-down at different levels of intensity.



Seismic equipment cabinets are designed, secured and braced specifically to withstand stresses imposed in the event of an earthquake.

These are tested in accordance with the FEM Method (finite-element methodology for modeling earthquake ground motion) to guarantee earthquake stability for Zone 4, with a load of up to 450kg (992lb) in compliance with the Telecordia Standard.

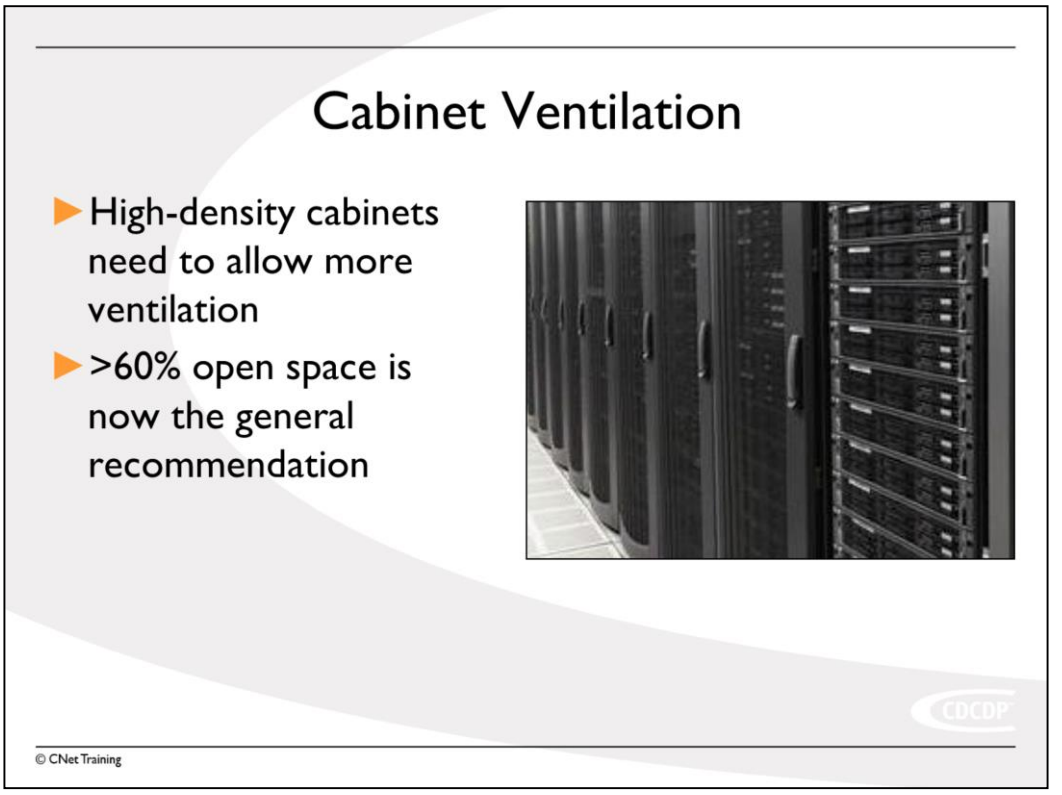
ISO-Base™ Seismic Isolation Platforms work by using the principle of base isolation to decouple seismic shock and vibration from equipment through the use of the patented Ball-N-Cone™ Technology. This eliminates or dramatically reduces the path on which damaging shock waves and vibrations can travel.

The ISO-Base™ Seismic Isolation Platform features a modular design which allows a multitude of configurations. ISO-Base™ Seismic Isolation Platforms consist of individual units called Planks; these are connected together to form a Seismic Isolation Platform. Each Plank has an identical top and bottom piece with Ball-N-Cone™ Isolators located in both the front and back of the plank.

Ball-N-Cone™ Isolators consist of two conical Stainless Steel dishes sandwiched over a steel ball bearing. This unique design allows the ISO-Base™ to roll smoothly and evenly while accepting input ground accelerations from any direction. Using gravity as a restoring force, the bearings inside the ISO-Base planks recentre themselves after an earthquake as the shaking decreases.

Two ISO-Base™ planks are connected together to form a platform for one cabinet. However, multi-unit rows of cabinets are also easily isolated because of its modular design.

http://www.worksafetech.com



Older cabinets had solid or glass doors. These are not suitable for equipment cabinets that generate lots of heat.

High power server cabinets need to allow open ventilation to the front of the equipment, and so should either have no front door at all, or have a highly-vented door to allow good airflow through the equipment.

Servers require the front and back cabinet doors to be at least **63%** open for adequate airflow. This can be accomplished by removing the doors, or by ensuring the doors have a perforated pattern that provides at least **63%** open area. In addition, maintain a minimum of 1.5in (3.8cm) clearance between the systems and front and back doors of a cabinet. (Source: Oracle)

One method of ensuring proper cooling is to specify a cabinet door that provides over 830 in^2 (0.53548 m^2) of ventilation area, or doors that have a perforation pattern that is at least **63%** open. (Source: APC)

Enterprise-class cabinets provide **65%** open ventilation using perforated front and rear door assemblies. To support newer high-performance equipment, glass doors must be removed from older HP cabinets and from any third-party cabinets. (Source: HP)

The cabinet should either have no doors or, if required for security, doors with a minimum **60%** open mesh for maximum airflow; it is best not to equip them with top-mounted fan kits. (Source: Chatsworth)

Ventilation through front and rear door perforations to provide a minimum of **63%** open space. Increasing the size and area of ventilation openings can increase the level of ventilation. (Source: BICSI)

Clearance and Accessibility

- A minimum of 1m (3ft 3in) of front clearance shall be provided for installation of equipment
  - 1.2m (4ft) is preferable to accommodate deeper equipment
- A minimum of 0.6m (2ft) of rear clearance shall be provided for service access at the rear of cabinets
  - 1m (3ft 3in) is preferable
- Some equipment may require service clearances of greater than 1m (3ft 3in)

© CNet Training

Clearance and Accessibility

UK

- **BS EN 50174-1** 'Information technology - Cabling installation specification and quality assurance' requires:
  - The minimum clearance on all faces of the frames and cabinets, where access is required, shall be 1.2m (4ft).
- All regulations need to be understood:
  - The Electricity at Work Regulations
  - The Building Regulations
  - Health & Safety at Work Act

© CNet Training

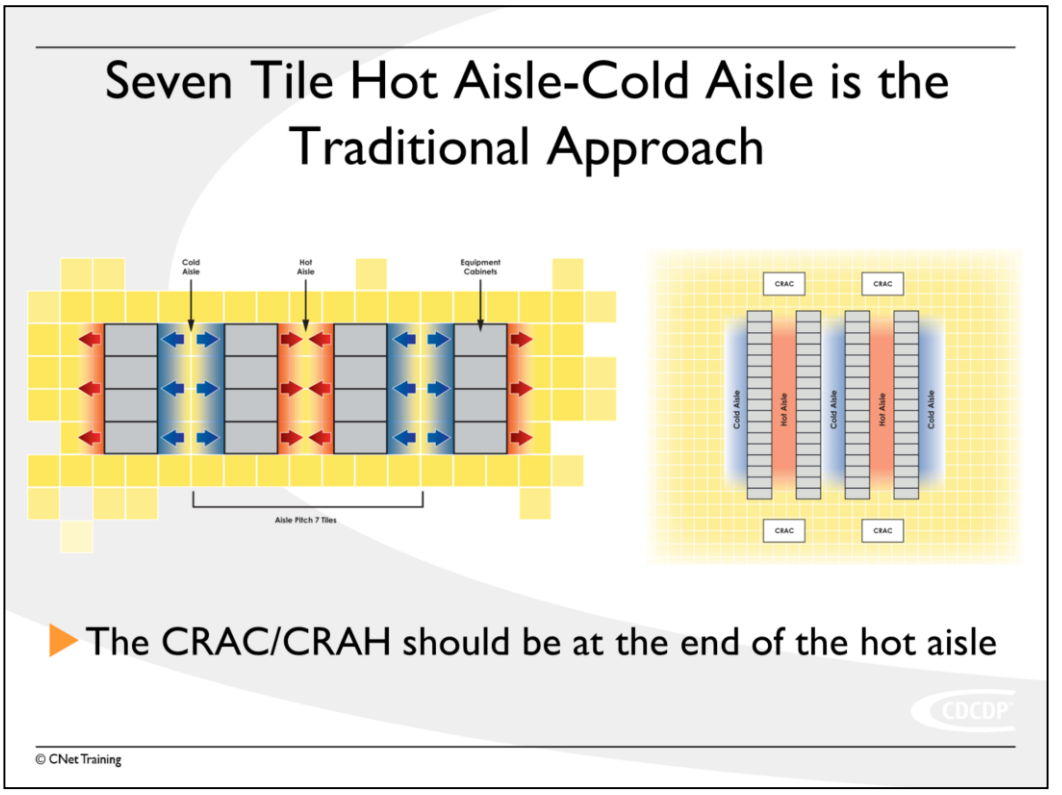
Clearance and Accessibility

USA

- BICSI 002 – Data Center Design & Implementation Best Practices:
  - The minimum width of an aisle shall be 0.9m (3ft), depending on local code requirements and voltage level present in cabinet
  - There should be at least a 1.2m (4ft) clearance at the front of racks and cabinets to permit unobstructed access, equipment movement, and maintenance
- TIA 569-C – Telecommunications Pathways and Spaces
  - Front clearance of 1m (3t) shall be provided for installation of equipment
  - Front clearance of 1.2m (4ft) is preferable to accommodate deeper equipment
  - Rear clearance of 0.6m (2ft) shall be provided for service access at the rear of racks and cabinets
  - Rear clearance of 1m (3ft) is preferable
- National and local codes apply

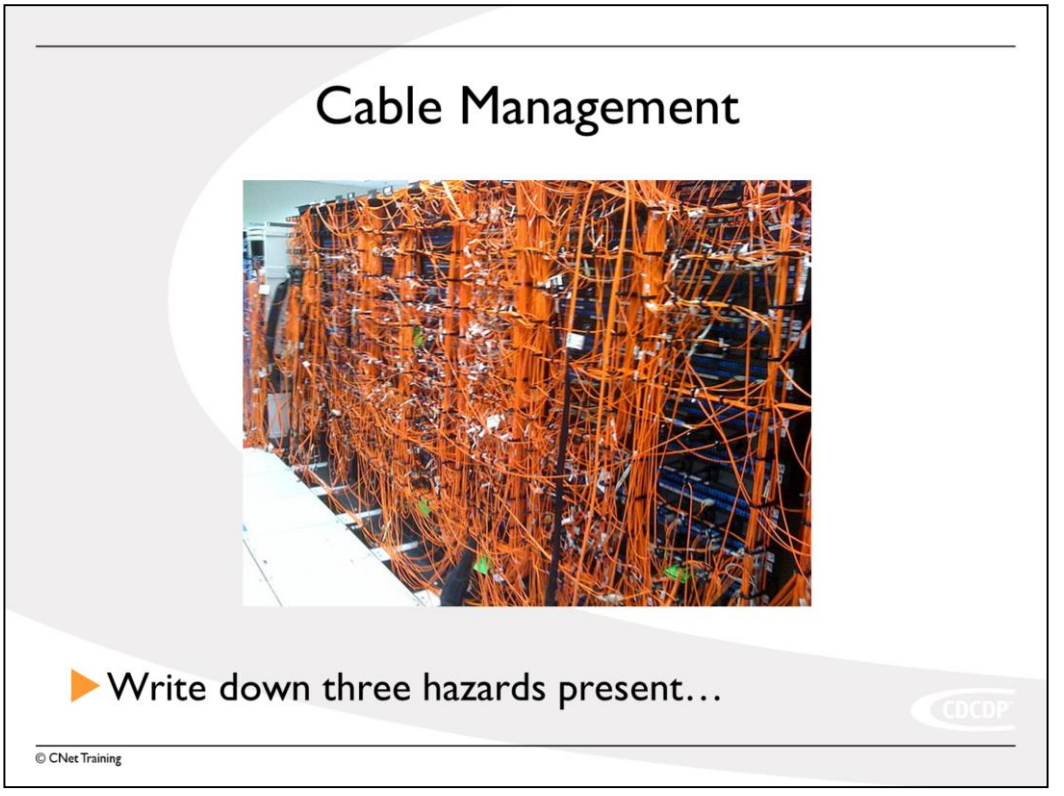
© CNet Training

The CDCD must be aware of all the respective local codes and regulations.



In the seven tile hot aisle-cold aisle model:

- The hot sides of adjacent rows face towards each other to create the hot aisle and, similarly, the cold sides create the cold aisle.
- Air conditioning units pump cold air into the floor void.
- Vents in the floor deliver cold air to the front of two lines of equipment cabinets facing each other – the cold aisle.
- Hot air escapes through the back of the cabinet into the hot aisle, where it returns to the air conditioning unit.



One purpose of a cabinet is to accommodate patchcords neatly. The sort of computer room shown above is an extreme example, but it demonstrates the point that some Data Centres have lapsed into this poor standard.

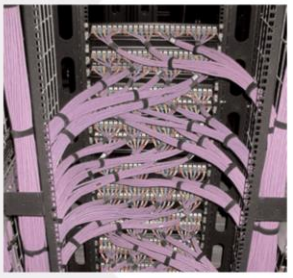
- Can you write down three hazards that the patchcord layout above will present?

Cable Management

- Are your three hazards present in this layout?
- Are there any new areas of concern?

© CNet Training

Cabling in the Cabinet/Rack



- Cable routing is generally at the sides to allow even air distribution within the cabinet
- Bend radius of cabling media must be properly assessed
- Note the brush seal in the floor and use of Velcro strapping
- Nicely done!

© CNet Training

Route cables away from airflow paths

- Can you identify issues with these pictures?

© CNet Training

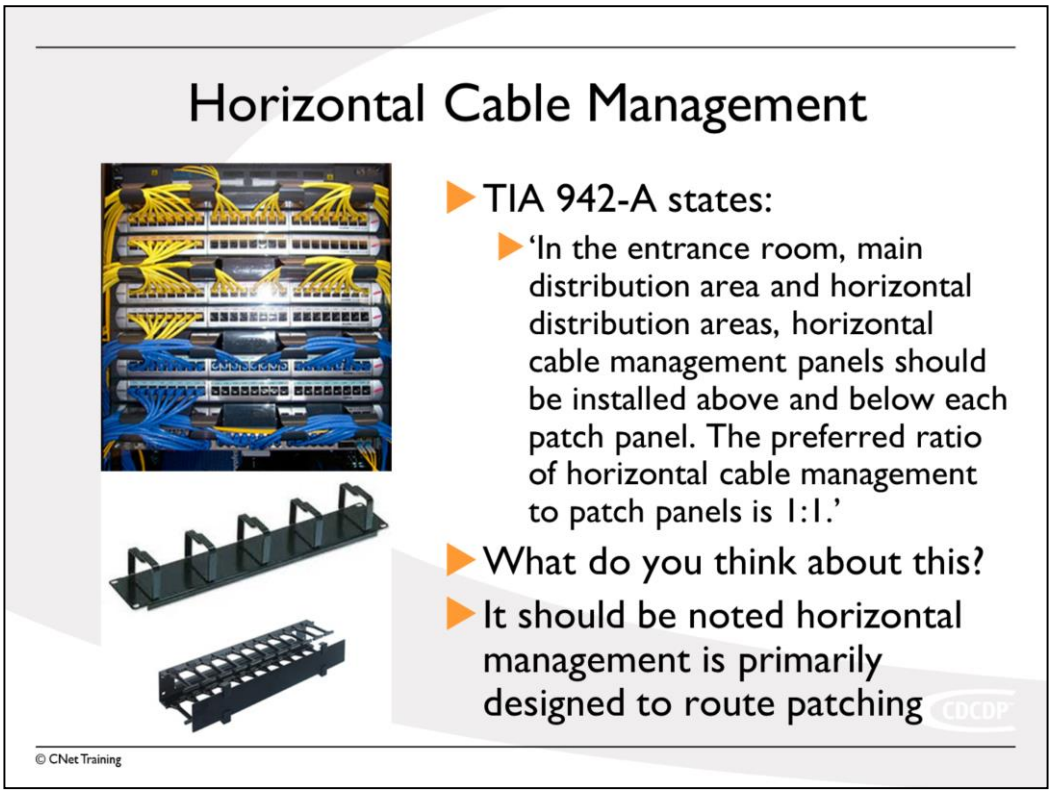
Cables can impede both the supply and return air temperature paths, so they must be routed correctly to minimise this effect.

Vertical Cable Management

- TIA 942-A states:
  - Vertical cable management shall be sized by calculating the maximum projected cable fill, including a minimum 50% growth factor
  - Where projected cable fill information is not available, consider deploying 250mm (10in) wide vertical cable managers
- These terms relate to one cabling design option
  - This does not necessarily work well with Cat 6a or Cat 7 due to the outer jacket size of the cables and their bend radius
  - Internal space planning is a key consideration

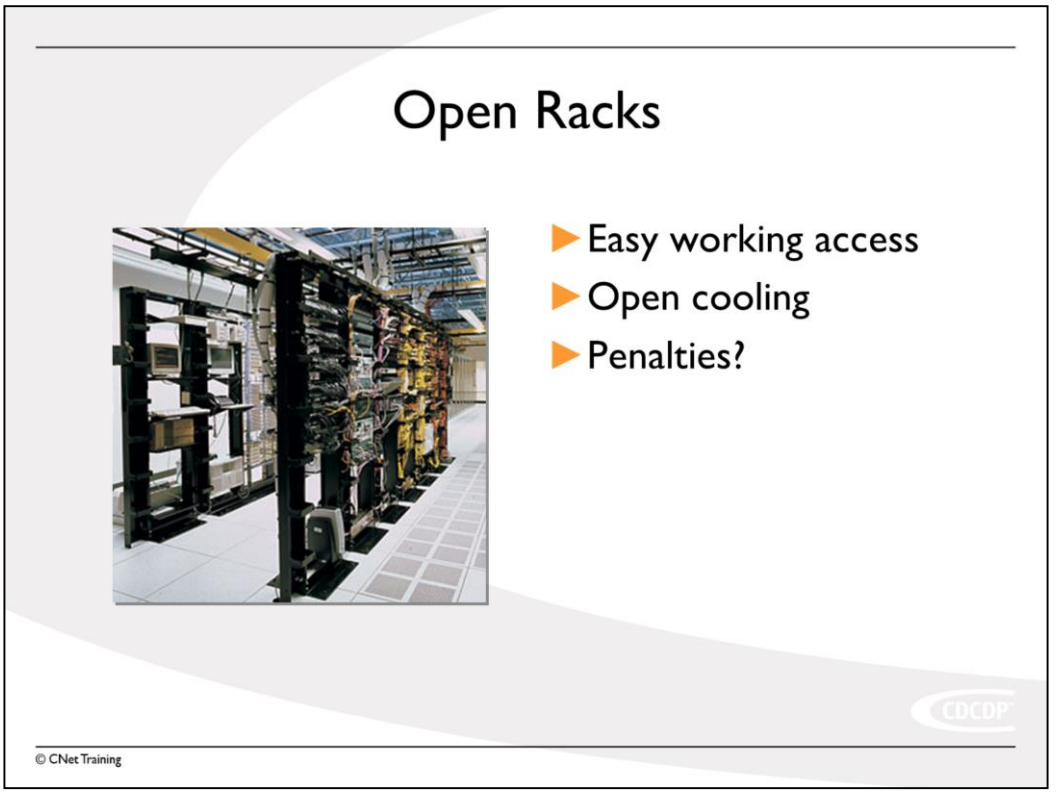
© CNet Training

There are some simple guidelines in TIA 942-A for good cable management. Sadly, these do not necessarily work well with Cat 6a or Cat 7 cable systems, due to their size and bend radius - the CDCD must consider internal cabinet space planning very carefully.



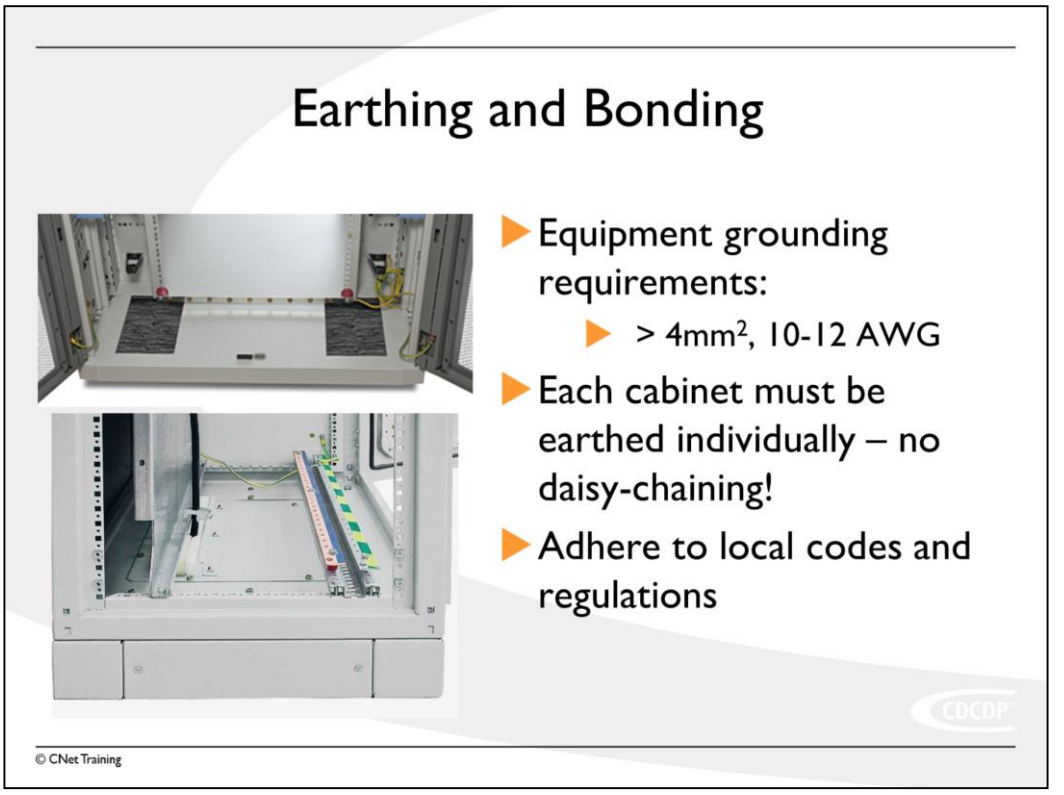
Fortunately, manufacturers make many accessories to manage cables and subsequently, many options for the CDCD to choose from. However, the CDCD must think through horizontal management requirements for each respective cable media, especially where optical cables are involved - ensuring the designated bend radius is not exceeded.

Do not leave the decision to the installer!



Some equipment can be installed on open racks.

On the face of it, this appears to be a simple option, but there are drawbacks and penalties associated with them.



If a circuit conductor is connected to earth or any other reference point, nothing which might reasonably present danger (by breaking electrical continuity or introducing high impedance) shall be placed in that conductor, unless suitable precautions are taken.

In practice, what this means in the Data Centre is that each cabinet must have a dedicated connection to a main earth terminal (MET), or to a suitable system reference potential plane (SRPP); daisy-chaining is not allowed. It also means the doors and side panels must all be electrically connected.

Design Issues

- Cable entry - Top or bottom?
- Securely mounted
- Equipment load capacity
- Cooling method
- Power supplies
- Earthed / grounded
- Cable management
- Blanking plates

© CNet Training

There are many aspects the CDCD must consider when selecting equipment cabinets to support design requirements.

Plan for Safety

- Ensure floor is strong enough
- Ensure floor is level and in good order
- Level the cabinet
- Put heavy equipment towards the bottom
- Bolt to floor whenever possible
- Follow national rules for seismic fixing kits
- Bolt the cabinets together with baying kits
- Correctly earth all the metalwork
- Meet local AHJ requirements

© CNet Training

Whichever cabinet is used, there are a number of simple guidelines that must be followed so the cabinet is installed safely.

Review

- Can you?
  - Appreciate the cabinet design considerations
  - Describe strategies for effective cabinet layouts

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 3

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

Power

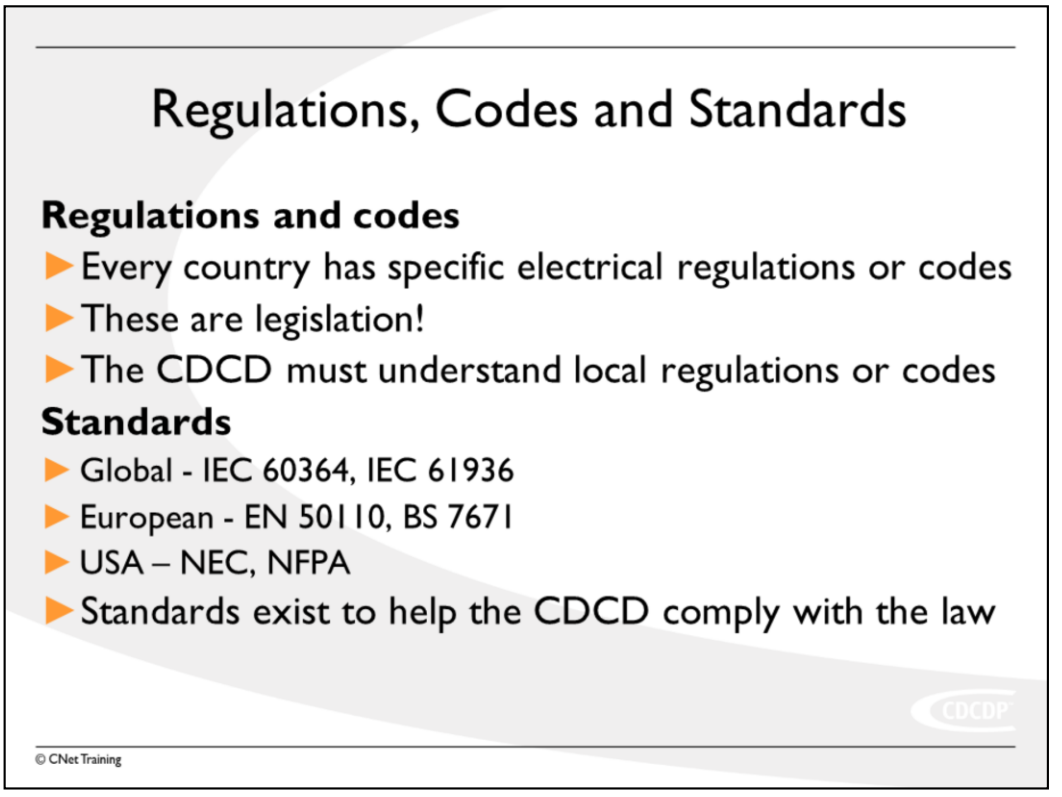
Version 1509

CDCDP

Objectives

- At the end of this module you will be able to:
  - Understand applicable regulations and codes
  - Identify where power is used
  - Identify key power components
  - Discuss power distribution options
  - Discuss emergency power off (EPO)

© CNet Training



Since other industries may be involved in the Data Centre design, the CDCD should also be knowledgeable about the related Standards, local and national regulations appropriate to the region.

Worldwide

IEC 60364 and 61936 contain common rules for electrical installations.

Europe

The European Standard EN 50110 'Operation of Electrical Installations' consists of two parts:

- EN 50110-1 contains minimum requirements valid for all CENELEC countries and some additional informative annexes dealing with safe working.
- EN 50110-2 is a set of normative annexes (one per country) which specify either the present safety requirements, or give the national supplements to achieve these minimum requirements.
- BS 7671 is the country variant for the UK which ensures compliance with the IEC and EN Standards.

USA

The National Electrical Code, NFPA codes and local codes apply. The CDCD needs to keep abreast of the latest discussions regarding codes and Standards, as they can often be wrongly (and expensively) applied. NEC 645 and NFPA 75 do not apply to all IT facilities, and may or may not apply to the new Data Centre, so the designer must determine the applicable codes at the outset.

The Language of the Power Engineer

- Volts, amps, ohms
- Watts, VA
- Direct Current (DC) and Alternating Current (AC)
- Voltage levels, Peak, RMS
- Crest / form factors
- 1-phase, 3-phase
- Lead, lag
- Resistance, inductance, capacitance, conductance
- Reactance, impedance
- Ohm's Law
- Kirchoff's Laws
- Joule's Law

CDCDP

© CNet Training

The CDCD needs to be able to understand the engineering language used by power engineers so they can have a meaningful discussion. We are not covering this in great detail here as it is one of the topics of the CDCDP course.

The Power Continuity Plan

- The CDCD needs to work with the Electrical Engineer to formulate a detailed power continuity plan to ensure power is maintained to the IT critical load under all applicable situations
- This must detail and document how the electrical network should operate under all conceivable situations
- It will cover all component parts of the power train to the IT equipment, including all main and standby systems

CDCDP

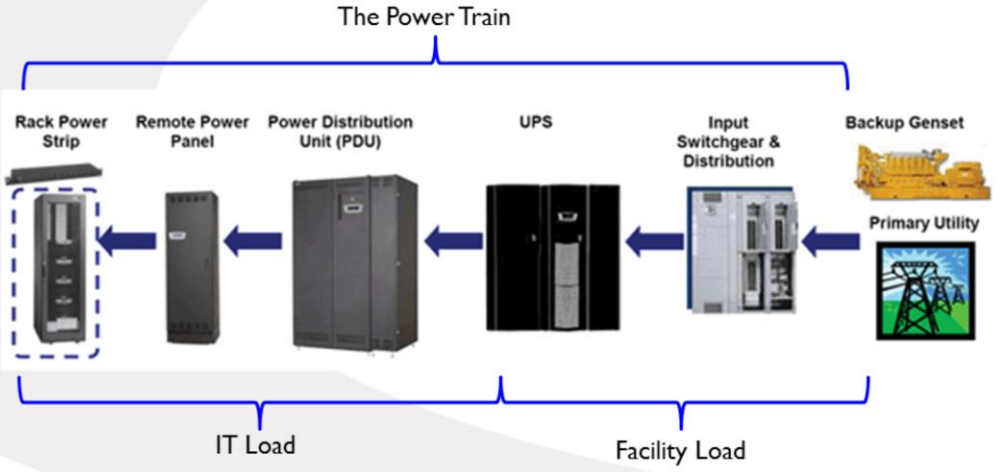
© CNet Training

The power continuity plan (PCP) will be prepared by the CDCD together with his electrical engineer. The PCP should account for all scenarios and ensure a comprehensive set of rules for all eventualities. Incorporating aspects such as:

- Clarification of the Day One load demand and future build-out expectation
- Whether it is a modular-based design or full Day One fit-out
- What are the designated availability, redundancy and resilience levels
- Designated load per cabinet and different environmental demands (A/B feeds)
- Built-in flexibility and scalability of the planned design
- Potential client demands (specific Service Level Agreements)

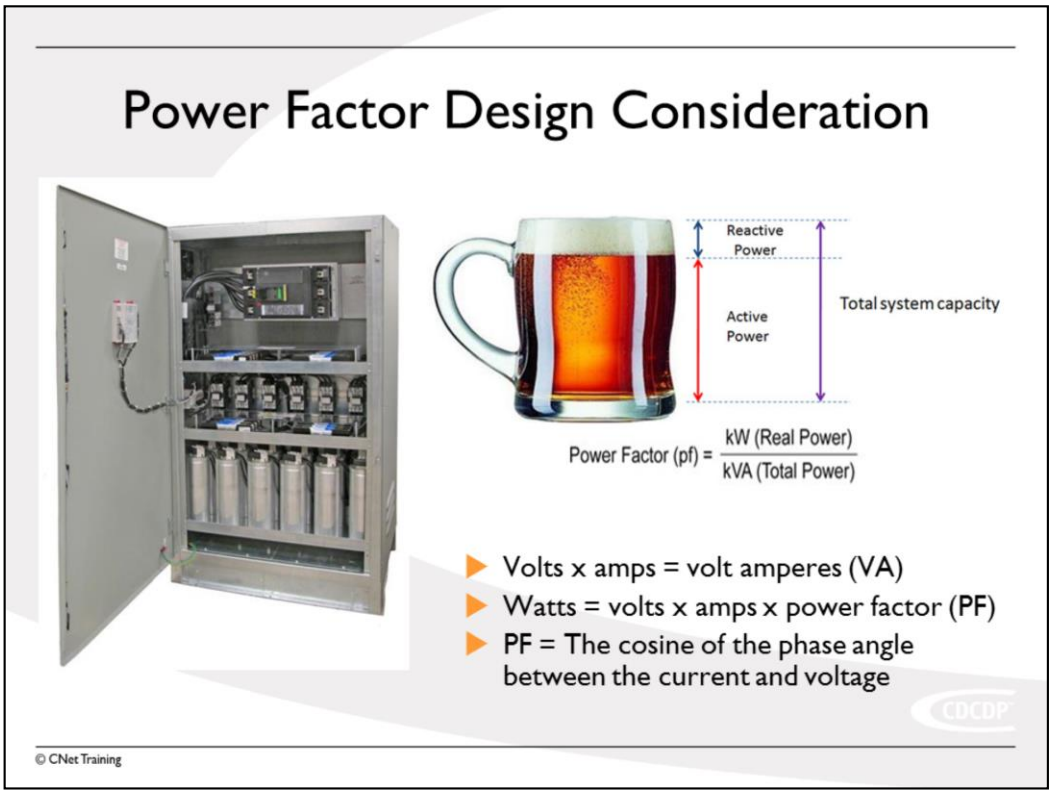
- What other factors can be provided by the CDCD?

The Data Centre Power Train



- Understanding the capabilities and limitations of the power infrastructure is a key necessity

© CNet Training

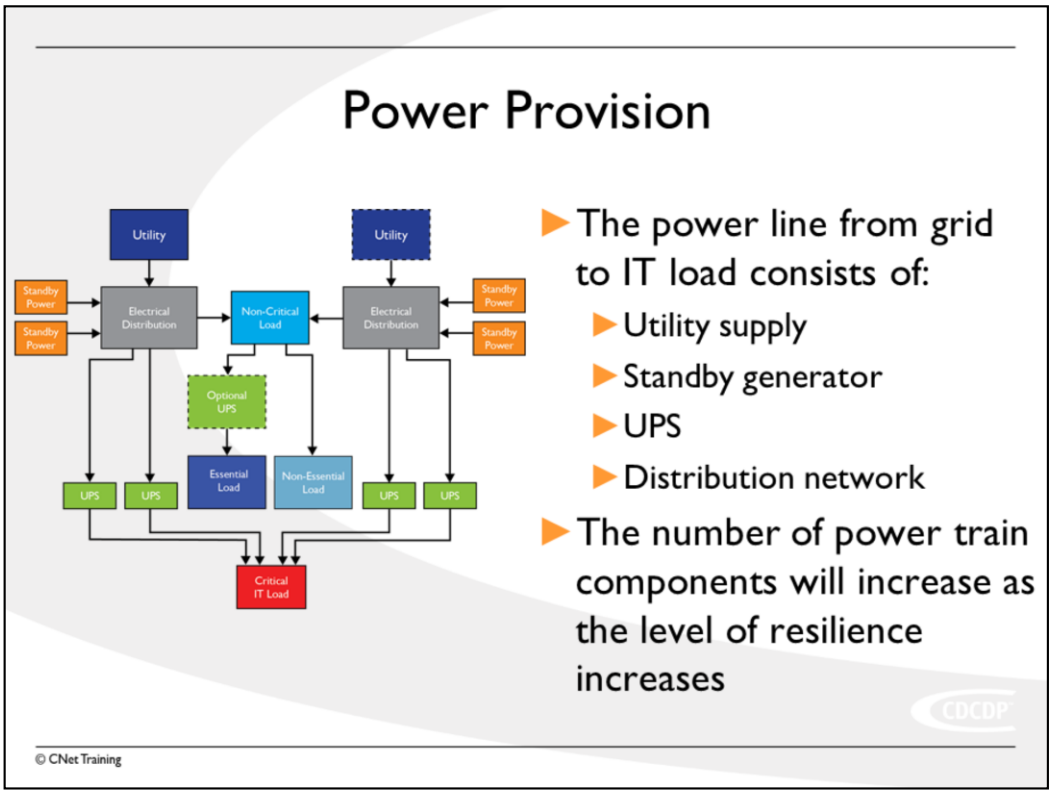


Electrical load like motors, transformers, cooling units, etc. require REACTIVE power to set up the magnetic field, while the ACTIVE power produces the useful work. Total Power is the vector sum of the two and represents what you pay for - i.e., kVA service capacity charge. Power Factor Correction (PFC) equipment provides the means of reducing reactive power being supplied by the utility. Reducing the reactive power supplied by the utility results in a cost reduction to electric bills, since kVA demand is also reduced.

An automatic PFC unit consists of a number of capacitors that are switched by means of contacts. These are controlled by a regulator that measures power factor in an electrical network. Depending on the load and power factor of the network, the power factor controller will switch the necessary blocks of capacitors in steps to make sure power factor stays above a selected value.

Ensuring a good Power Factor has numerous energy efficiency benefits:

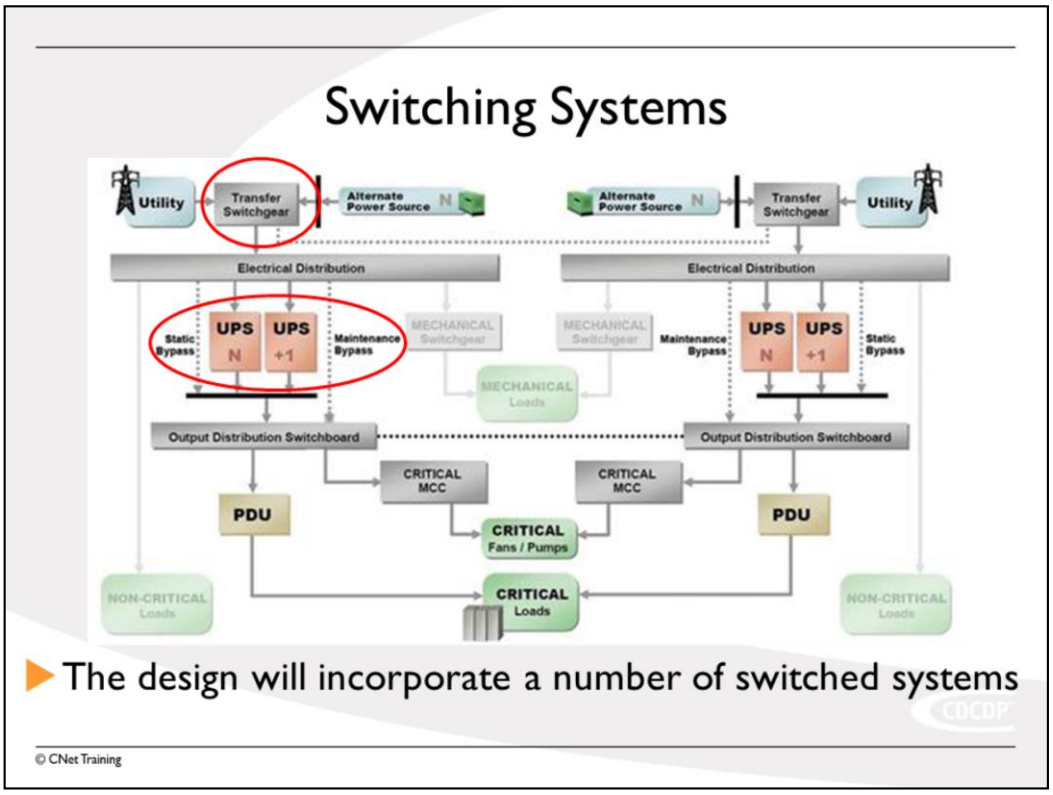
- Environmental benefit, reduction of power consumption by improved energy efficiency
- Reduced power consumption means fewer greenhouse gas emissions and fossil fuel depletion by power stations
- Reduction of electricity bills
- Extra kVA available from the existing supply
- Reduction of losses in transformers and distribution equipment
- Reduction of voltage drop in long cable runs
- Extended equipment life
- Reduced electrical burden on cables and electrical components



Remember this from before? What sort of power continuity plan will be required here?

Now we will talk about some of the components.

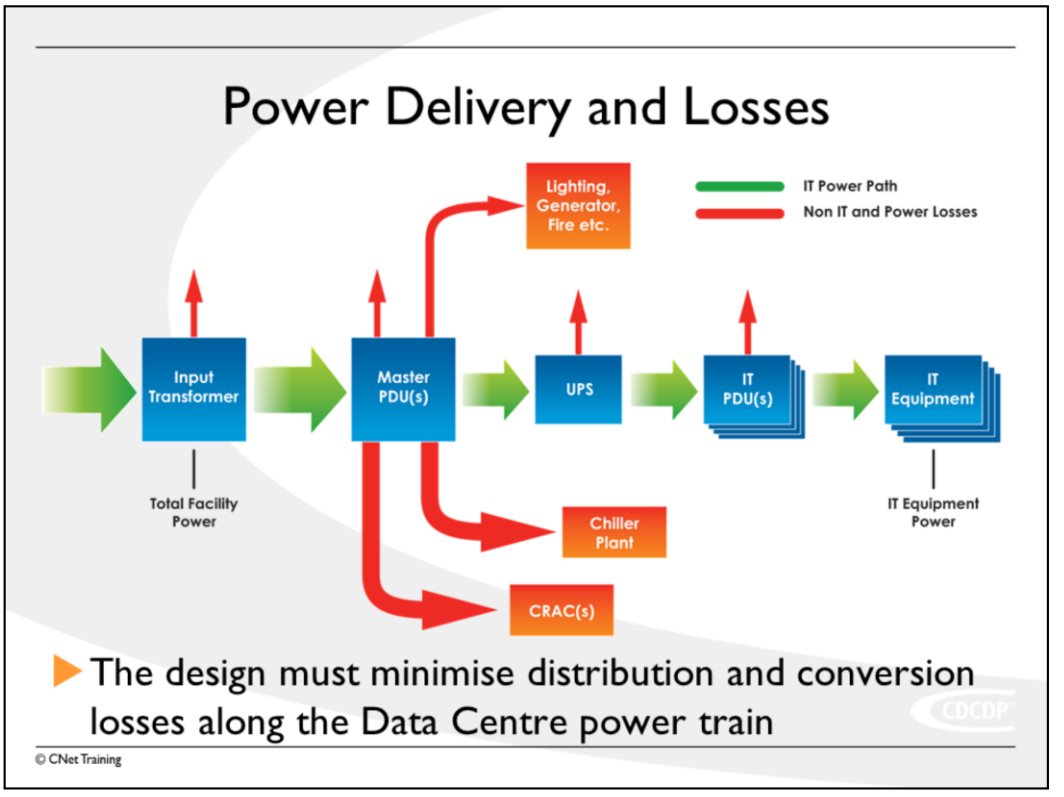
Note: The above schematic is an illustration of a power infrastructure for a Fault Tolerant Data Centre



The power infrastructure must be able to support the mission critical environments of the Data Centre under all applicable situations; this includes the ability to switch to standby systems in the event of a failure, or to enable operational maintenance to be undertaken. This incorporates key switching systems such as:

- Automatic Transfer Switch (ATS)
- Static Transfer Switch (STS)
- Maintenance Bypass Switch
- Static Bypass Switch

These switching systems will be broken down in more detail within the Professional element of the CDCDP.

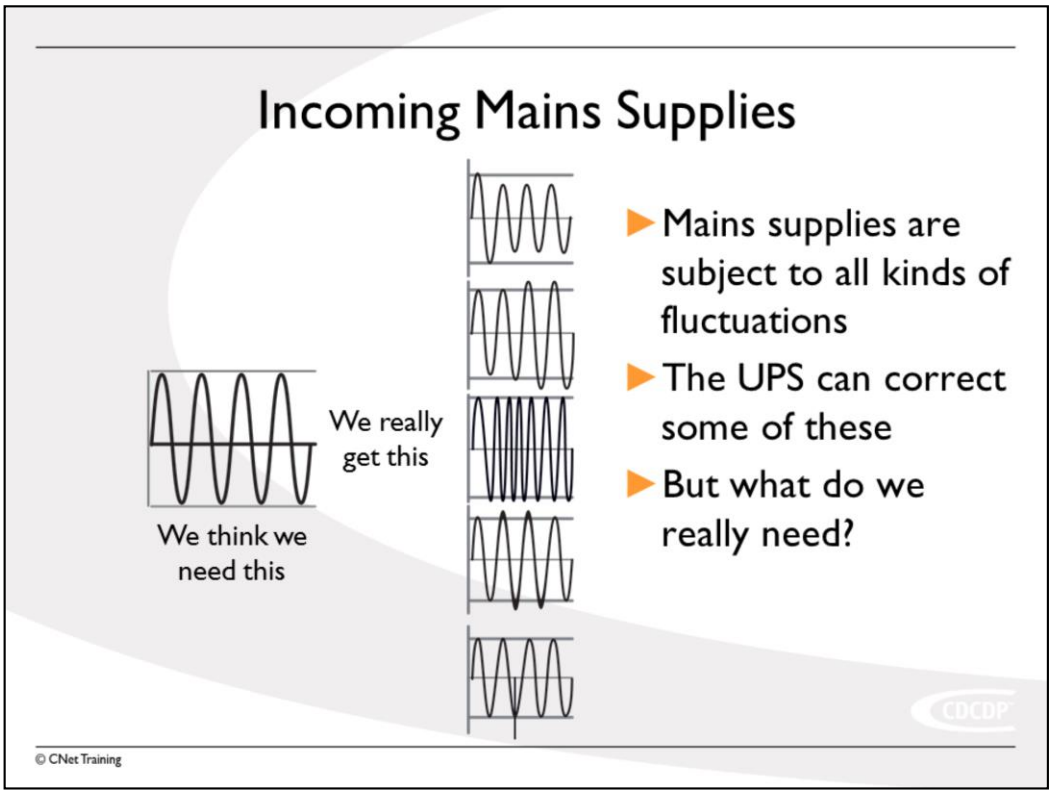


The Data Centre is a complex environment designed to house IT equipment. Utility power entering the Data Centre has to pass through a number of stages of voltage transformation, distribution and cleaning before finally being delivered to the IT equipment. Most of the power used within the facility is converted to heat, requiring significant cooling system capacity, which draws an additional load in a traditional, recirculating air Data Centre. There are also a number of ancillary support systems in the Data Centre, such as lighting, generator pre-heaters, fire suppression systems, and occupied areas which also require electrical power.

The slide shows a simplified representation of the power delivery and loss path in a Data Centre.

Utility power enters the building on the left and passes through the power delivery chain to the IT equipment on the right. Each stage in the delivery chain has inherent losses, shown by red arrows, as well as specific overheads shown as distinct paths.

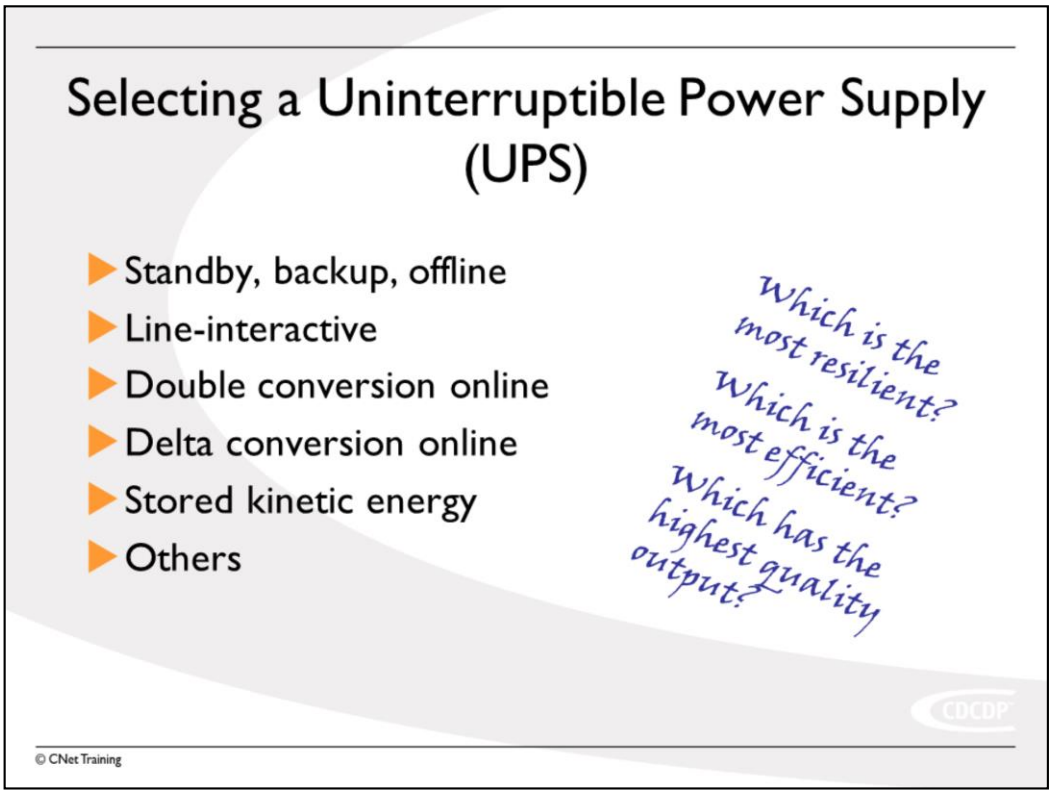
The actual implementation of a Data Centre is considerably more complex than this diagram suggests, and details such as whether CRAC units are fed from UPS may vary.



Ideally, we think we get a smooth and regular sine wave voltage from the utility company. In reality, mains incoming supplies can have all sorts of voltage and frequency fluctuations, depending upon the supply network and other loads in the vicinity.

The key question is - what do we really need?

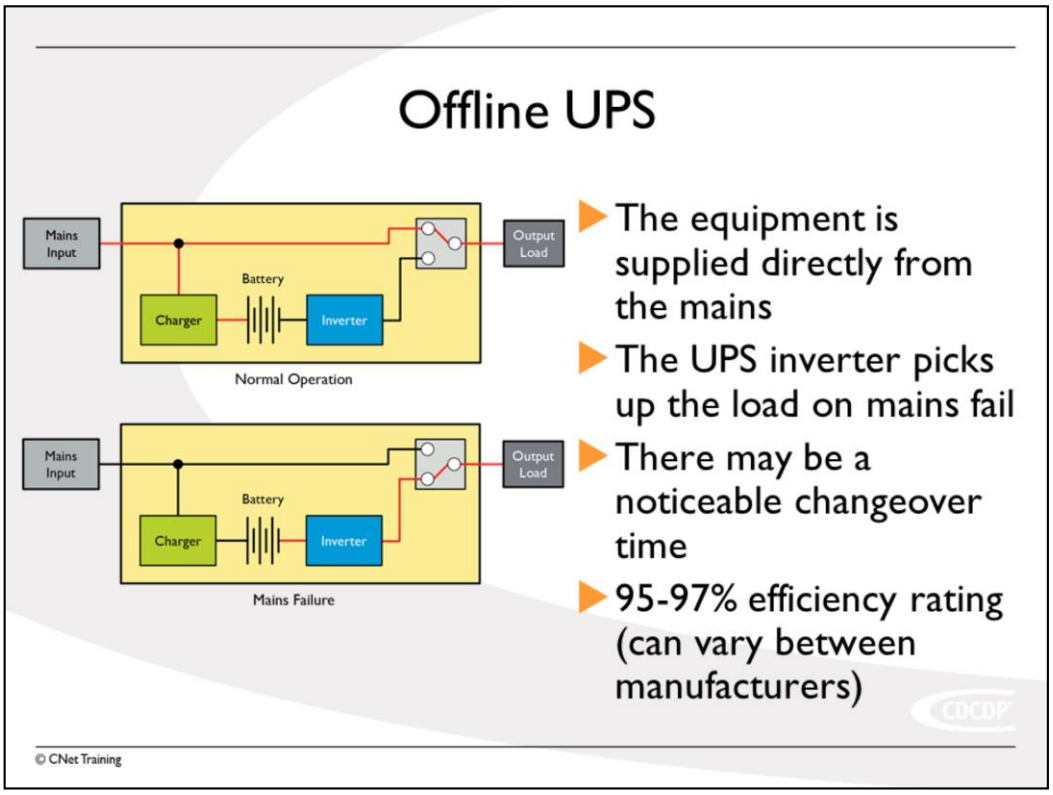
What will affect the profile and performance of incoming power?



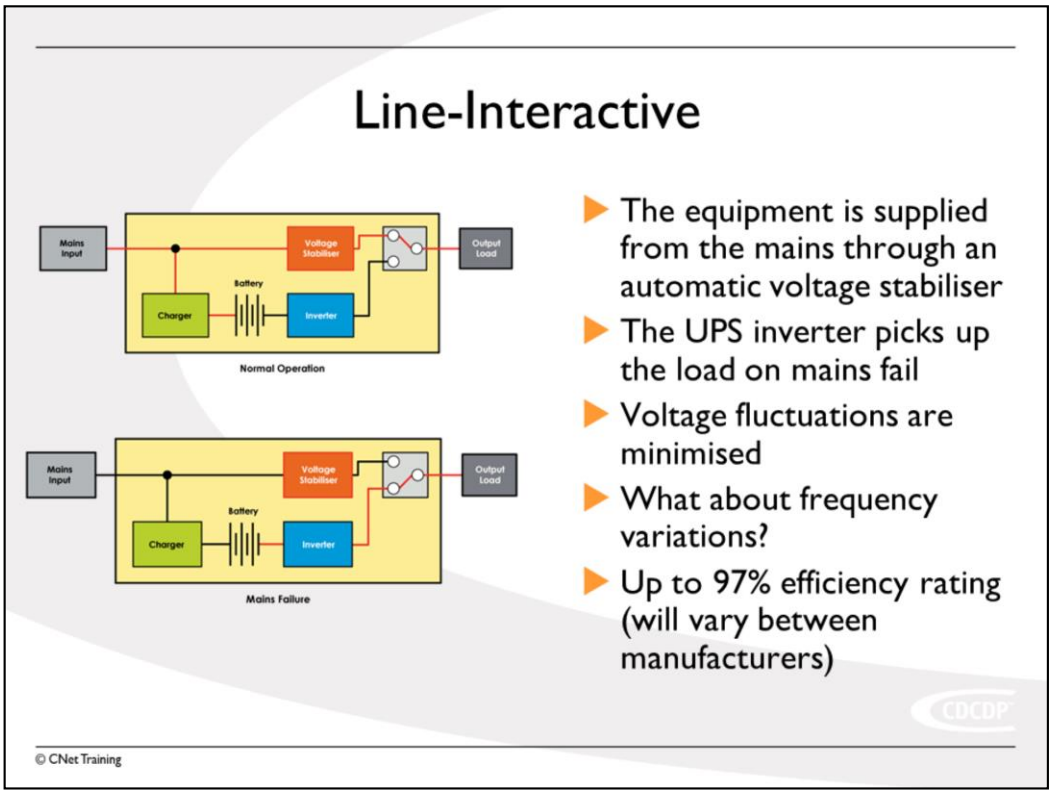
UPSs come in many flavours: Some are more resilient, while others are more efficient; some have a cleaner output - the choice is down to application and budget.

IEC 62040-3: Method of specifying the performance and test requirements, provides guidance for selection of the three types of UPS:

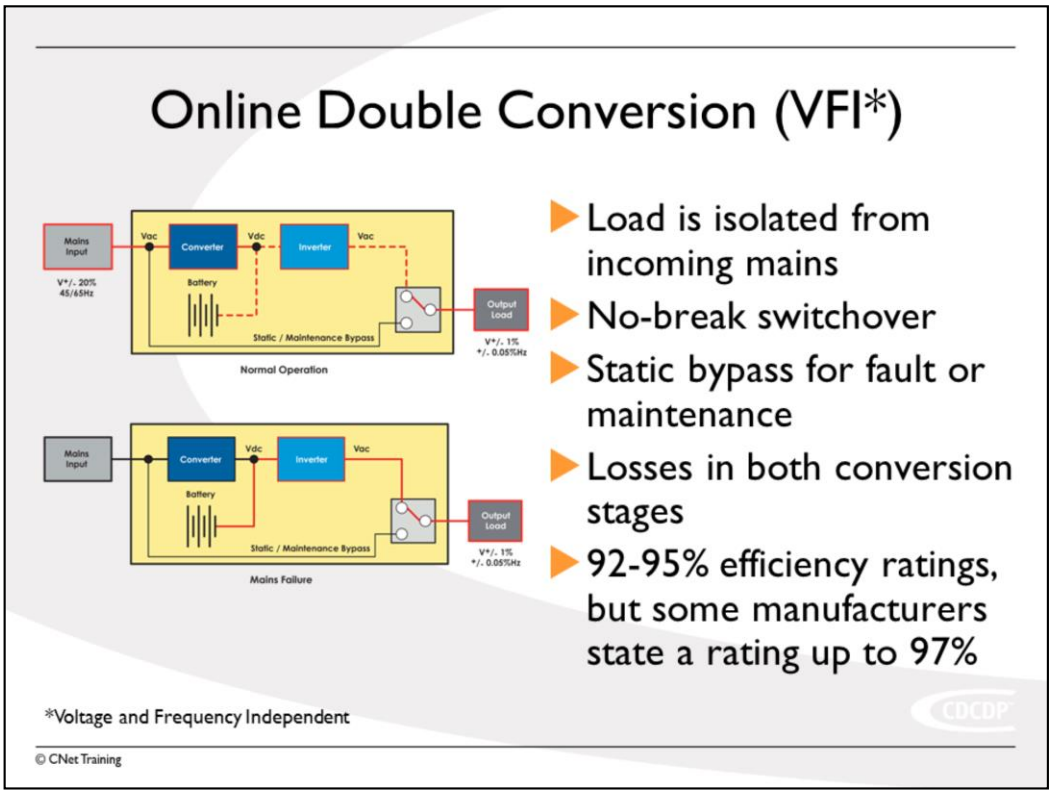
- Passive standby (Offline)
- Line–interactive
- Double conversion



- Offline systems are the simplest type of UPS.
- Under normal circumstances, the battery is charged from the incoming supply.
- Under mains failure, the battery continues to supply the load via the inverter. It can take several milliseconds to change over, so there is a noticeable power interruption.
- Offline UPSs cannot correct mains voltage fluctuations, which may cause it to change mode *each time* an under-voltage occurs. This reduces battery lifetime due to frequent discharges.
- They cannot correct mains frequency deviations.
- Offline systems are mainly used for low power installations, such as small offices and other less critical applications, where riding through around 90% of power failures is good enough.



- Line-interactive devices appear similar to offline UPS, working directly from mains and switching to the inverter in the event of an outage.
- Line-interactive UPSs have automatic voltage stabilisation (which is often transformer-based) between the mains input and the transfer switch. This keeps the output voltage within a tight tolerance band required for correct operation of IT equipment. This feature eliminates the inverter 'kicking in' and discharging batteries at low mains voltage, increasing system reliability and battery lifetime.
- The output voltage is generally sinusoidal.
- Line-interactive UPSs cannot correct frequency and should be avoided on sites with small standby generators, which tend to have poor frequency regulation.

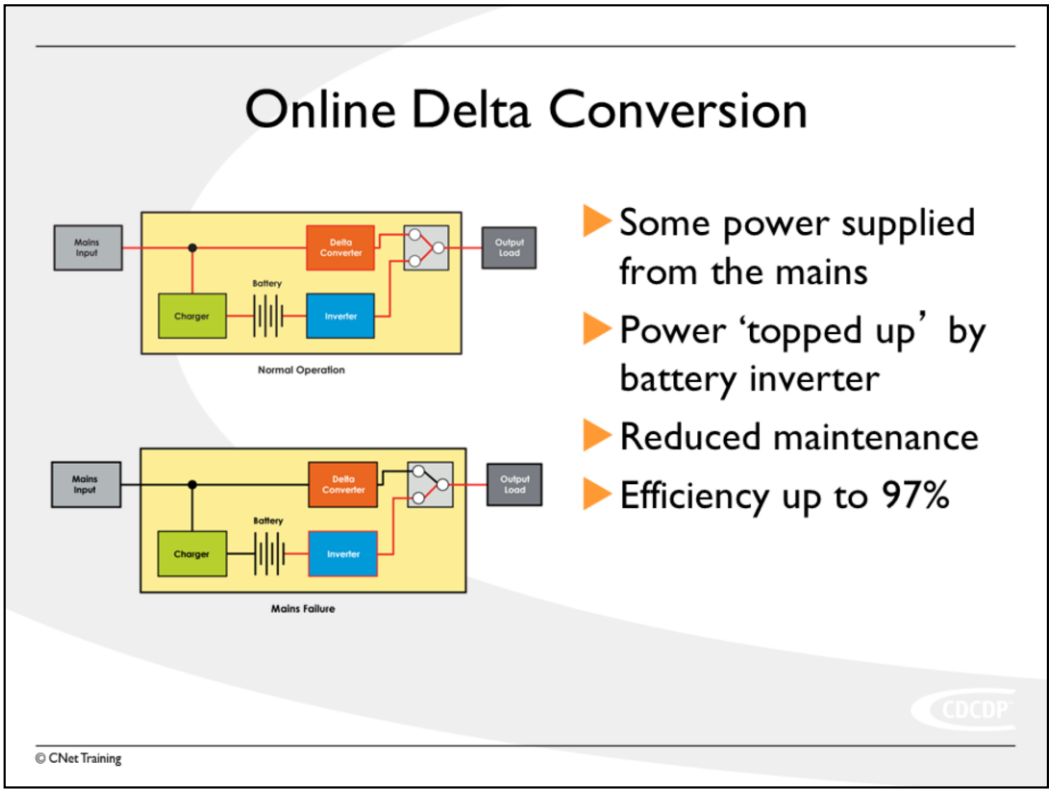


- Online systems comprise two conversion stages: The first stage rectifies the incoming alternating current (AC) power to direct current (DC), thus creating a DC bus which keeps the battery charged in normal operation. The inverter then converts the DC power back to AC in order to feed the critical load. This isolates the IT load from the incoming supply and removes the effects of voltage and frequency fluctuations.
- There is no interruption during switchover. This makes it ideal for Data Centre loads. However, there are losses in both conversion stages.
- The bypass is provided to enable maintenance on the UPS system, or to backup the UPS in case of malfunction. The transfer switch can automatically transfer the load to bypass in case of a UPS overload or failure.
- In normal operation, load energy comes from mains via the rectifier and inverter. Upon mains outage, the battery supplies the energy (which the load requires) by the DC/AC inverter. Should the mains voltage return before the battery is fully discharged, the rectifier will feed the load through the inverter and start a battery recharge regime to compensate for lost charge. Otherwise, the UPS will turn off when the battery becomes fully discharged.

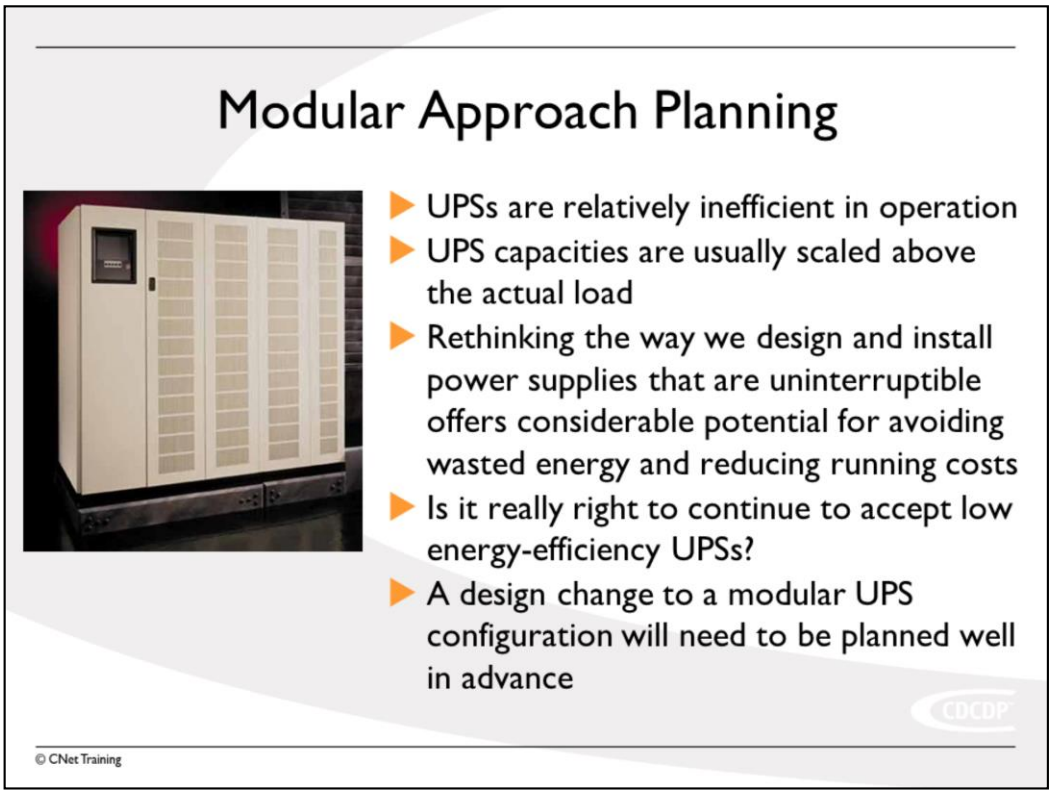
The UPS will automatically resume normal operation upon mains restoration. The rectifier will then feed the load via the inverter, recharging the battery. The output voltage of an online UPS is generally stabilised within 1% tolerance. Output frequency can be set by a free-running, crystal-controlled clock, allowing the online system to act as a frequency converter.

The merits of the double conversion online system have made it the preferred choice in spite of the capital and electricity costs.

- They protect against all types of mains disturbances
- They are available in a wide range of sizes
- Batteries can be added to increase the protected time
- Units can be modular and connected in a redundant configuration for resilience
- They have other features, and can work from generators, supporting a range of power factor loads



- Delta Conversion UPSs supply a portion of the load from the mains via the delta converter.
- The charger keeps the battery topped up and the inverter adds the remaining power to the load in order to stabilise output voltage within tight tolerances. The battery and inverter pick up the full load in the event of a mains failure.
- It has better efficiency than the online dual conversion system but, like the line-interactive UPS, it cannot correct frequency in this configuration.



Modular topology provides secure power with high availability and efficiency – and it does it cost-effectively too. Although the initial capital cost of a modular system is typically 10 – 15% above that of the standalone equivalent, the picture changes when Total Cost of Ownership (TCO) is taken into account. Improved energy efficiency, as well as other savings, mean the modular system's extra cost will be recovered within its first year of operation. Longer-term costs will also favour the modular system.

Module-level replacement reduces training costs as well as repair times. Repair-by-swapping can be performed by less-skilled or less-trained technicians than is necessary for component-level diagnosis and repair. By contrast, technicians responsible for maintaining standalone systems will typically not only require more in-depth knowledge, they must also extend this knowledge to cover different systems of varying designs. Eliminating the need for specialist UPS technicians and training can save up to 67% of the operational budget.

TCO for a modular system during its first year of operation can typically provide a 15% cost reduction compared to standalone systems. This figure includes the modular system's higher initial purchase price, and shows why modular systems make sound economic sense. Attractive as the cost savings are, there are other equally important reasons for choosing this topology: The first is the extremely high availability arising from significantly reduced repair time, a fundamental consideration for any UPS purchaser. The reduced floor space requirement and the flexibility to adapt quickly to changing critical load demands will also be attractive to many equipment operators. **Source: Kohler Power**

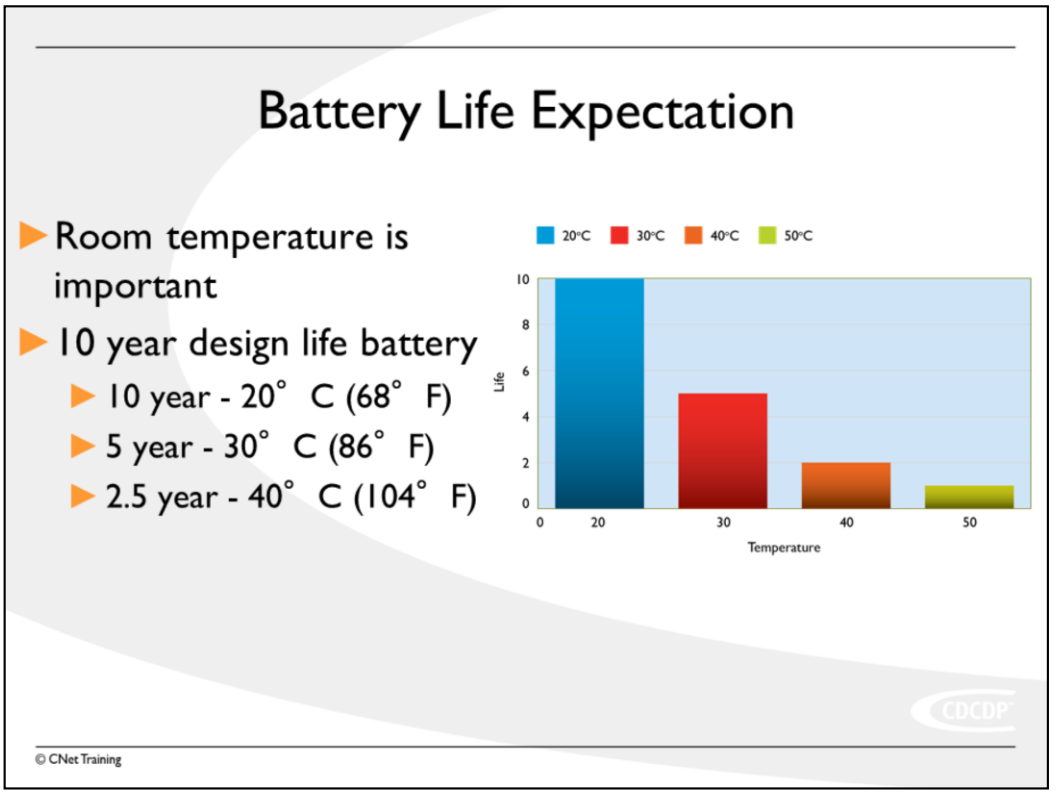
How Long Should Batteries Last?

- TIA 942-A 5-15 minutes
  - Further broken down against
  - TIA 942-A classifications:
    - Level 1 5 min (minimum)
    - Level 2 7 min (minimum)
    - Level 3 10 min (minimum)
    - Level 4 15 min (minimum)
- Sun / Oracle: 15 min
- US Army: 15 min (typical)
- Ultimately, the duration comes down to a business decision

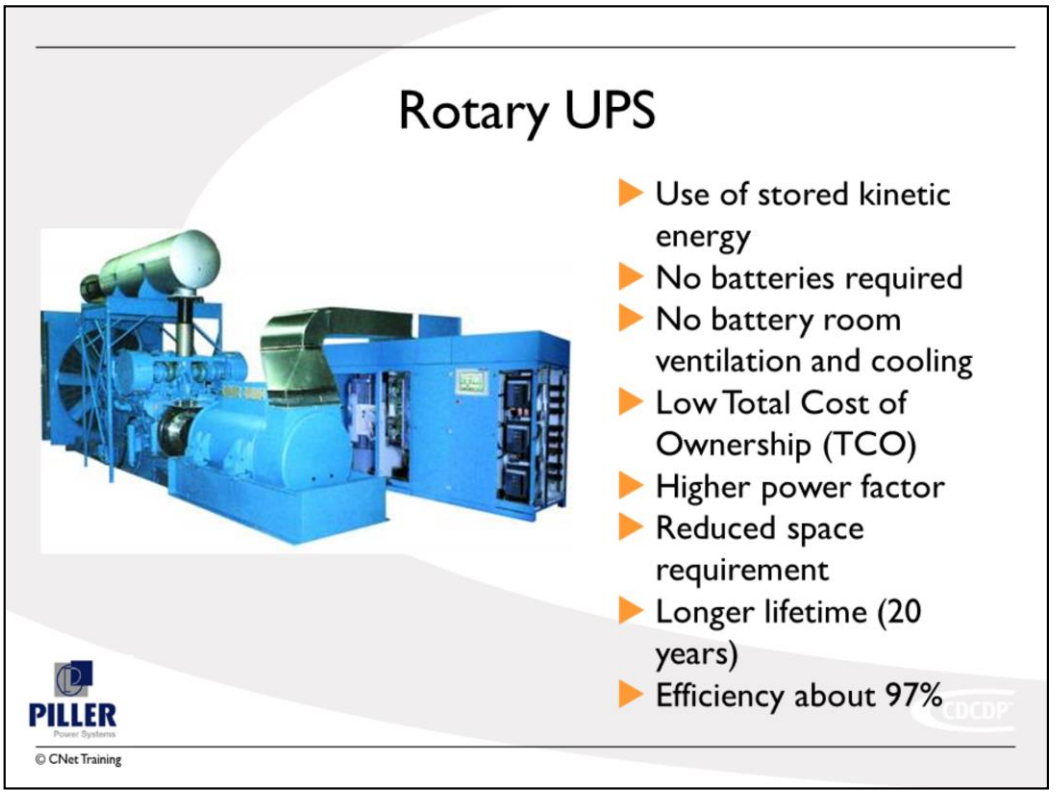
© CNet Training

These UPS systems employ batteries to store energy. There are recommended battery load / run times in the Standards; the CDCD must consider the best option to the business. Some of these are historic, as the UPS only needs to maintain the load until the generator picks it up.

Batteries can be large and heavy - keeping them constantly charged uses electricity; the amount of maintenance needed (and associated costs) should be kept in mind.



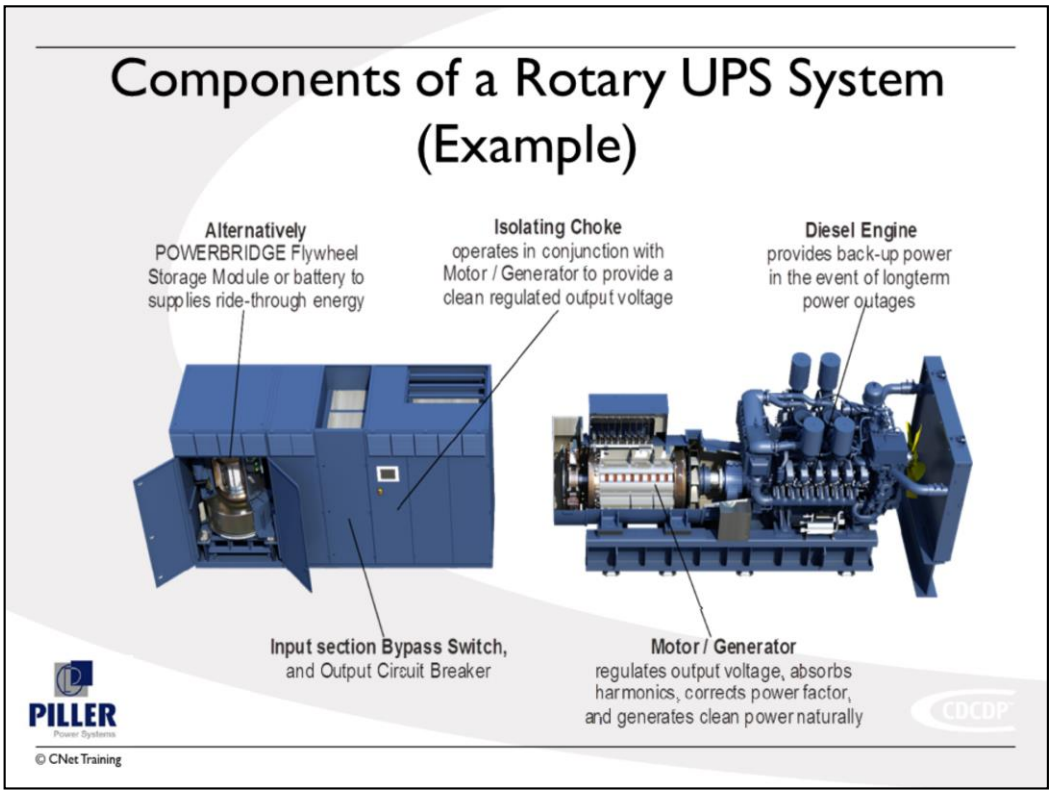
Batteries have their own requirements - ventilation and temperature can have a dramatic impact on their useful life. Those demands will increase proportionally to the number of cells needed to meet the operational requirement.



- For a UPS to be classified as a **rotary UPS**, its output supply must be connected to the windings of a rotating, synchronous generator.
- The simple construction of a rotary UPS and its electrical characteristics make it well-suited to large, highly-resilient applications where peak performance is paramount.
- The design life (typically 20 years) and high efficiencies (up to 97%) ensure rotary UPSs offer the lowest Total Cost of Ownership.
- RUPS and DRUPS configurations provide a wide range of options, depending upon individual requirements.
- The ability to avoid battery systems and the dynamic performance of kinetic energy storage devices offer a wide range of benefits which should be considered in the initial design of any mission critical system.

ALL ROTARY UPSs ARE NOT THE SAME – AN APPRECIATION OF THE DIFFERENCES CAN ONLY IMPROVE THE SELECTION OF BEST-FIT TECHNOLOGY FOR MISSION CRITICAL APPLICATIONS

Source: Piller

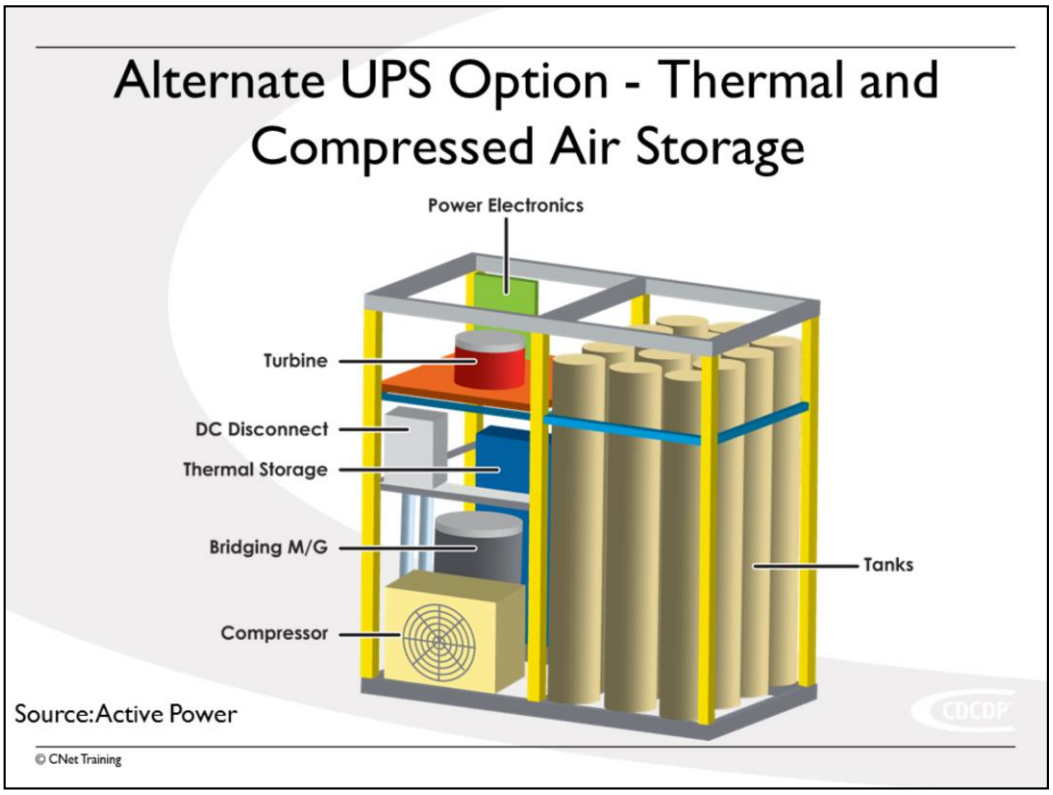


Correcting some common UPS misconceptions

- It must be a rotary UPS as it contains elements that rotate = WRONG!
- It is a rotary UPS and therefore requires a diesel engine = WRONG!
- It can't be a rotary UPS as it has batteries = WRONG!
- I can't use a rotary UPS as I need an LV solution = WRONG!
- I would like to use rotary but I need VFI mode of operation = WRONG!

<u>The Key Definition</u>:

In a Rotary UPS, the output voltage is generated within the windings of a rotating, synchronous generator or motor/generator



- Another way of storing energy for the UPS is to use compressed air. Thermal and compressed air storage (TACAS) systems are starting to appear in some Data Centres, typically providing power to a row of equipment racks.
- As well as providing backup power, these systems also produce cool (17°C/59°F) air as a by product, which can help maintain Data Centre temperature during a power outage.
- Sizes up to around 200kVA, with runtimes up to 45 minutes mean these could be used for smaller Data Centres with no generator for extended power backup.
- TACAS energy storage depends on both air temperature and air pressure, so the actual runtime depends on the number of storage tanks in the system.

Alternate UPS Option – Hydrogen Backup Power

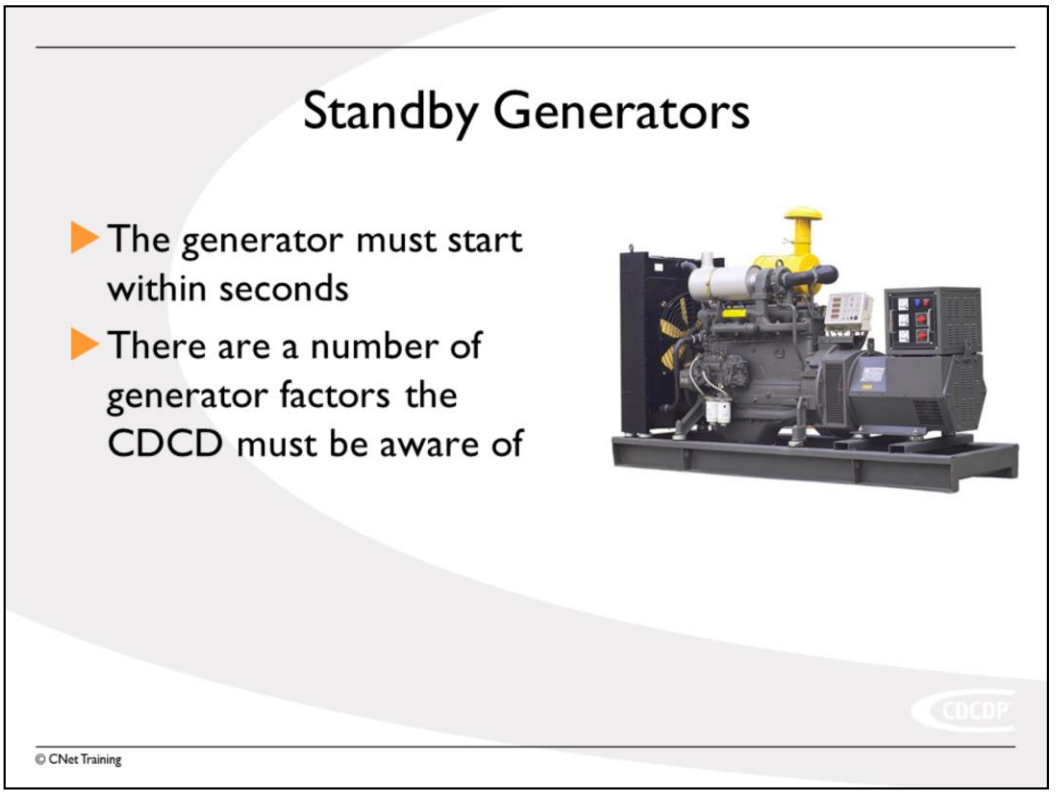
- Provides 16 hours of reliable backup power
- Converts chemical energy directly to electrical energy
- Highly efficient with reduced maintenance demand
- Environmentally friendly
- Smaller footprint
- Ideal for small to medium sized enterprises

COMMSCOPE

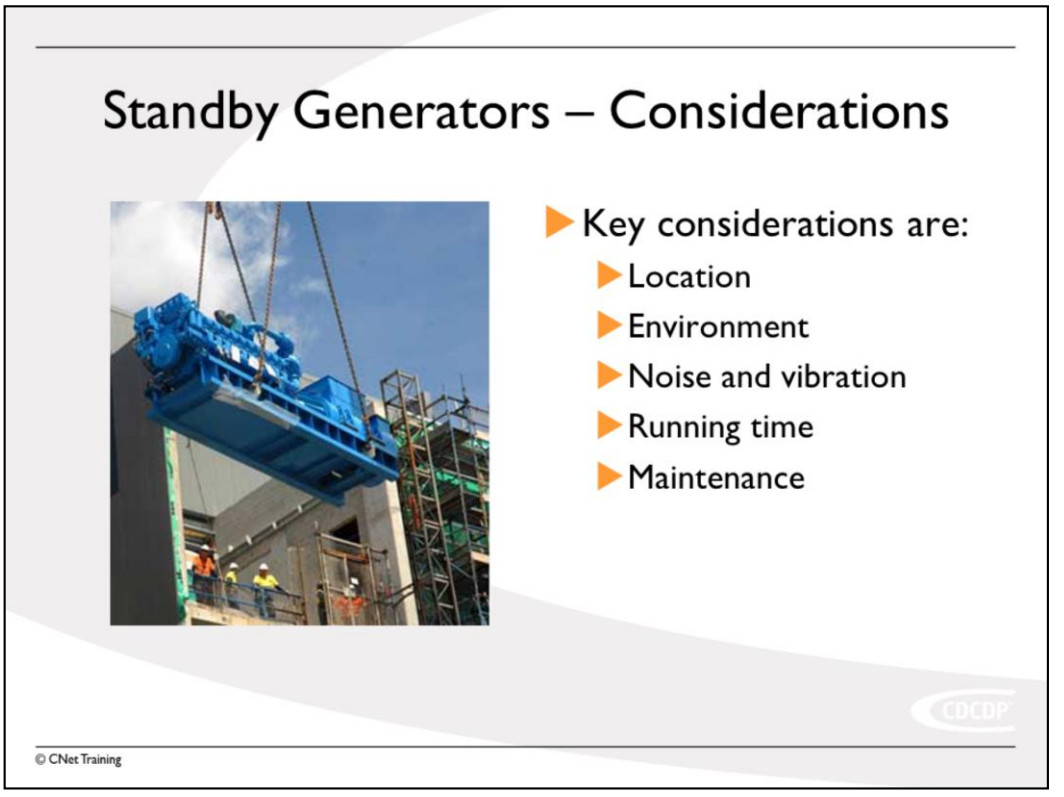
© CNet Training

CDCDP

- The outdoor cabinet fuel cell solution can provide up to 16 hours of reliable, environmentally-friendly backup power to enterprise core business computing systems
- The hydrogen fuel cell solution converts chemical energy directly to electrical energy without combustion. The system provides highly efficient, reliable and uninterrupted backup power for commercial building systems without the need for costly regular maintenance.
- It does not emit any greenhouse gases - the only by-products are heat and a small amount of water.
- The proton exchange membrane hydrogen fuel cells are housed inside an outdoor, environmentally-secure cabinet (roughly the size of a phone booth) with a smaller footprint than other solutions currently available on the market.



Most Data Centres have standby generator sets, which are usually diesel powered. It is necessary to maintain the generator so it will start within seconds when required. This requires regular maintenance and means the engine needs to be kept in a state of readiness.



The CDCD should be aware that generators need to meet a number of requirements that may not be obvious at first glance.

Obviously, the generator must start and pick up the load when necessary, which places demands on its location, environment and maintenance needs. However, there are many other external requirements that may be driven by local codes and regulations, including noise and exhaust emissions, which may affect the times it can be run.

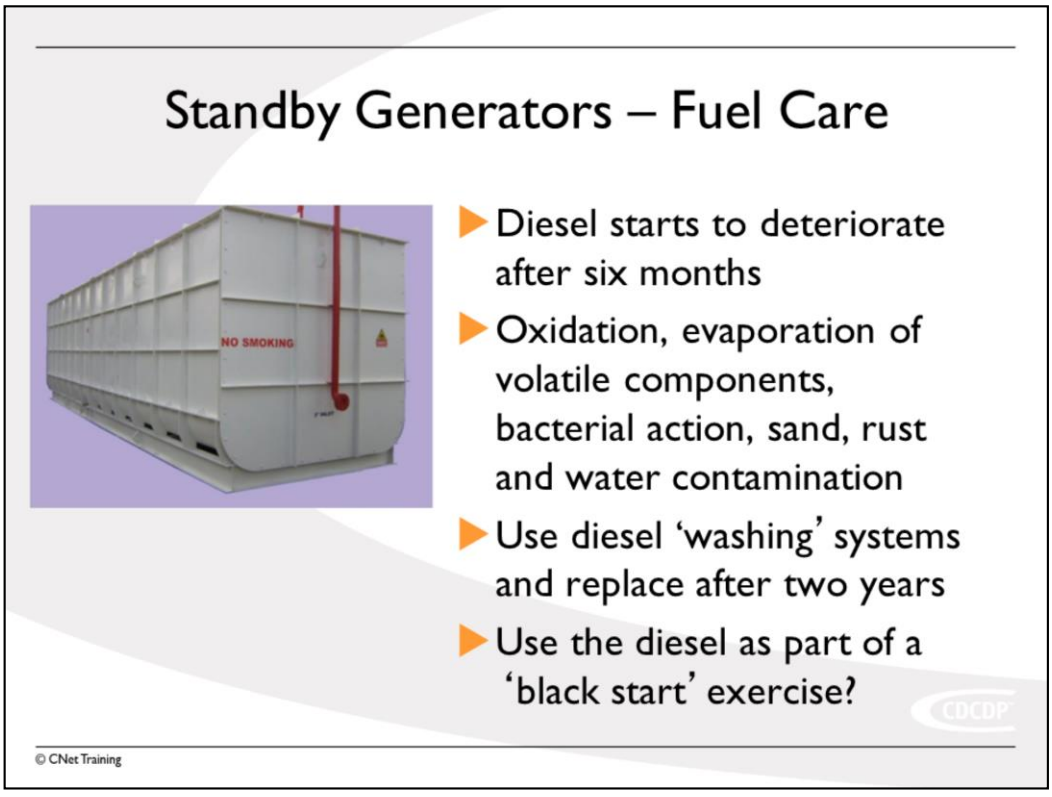
Standby Generators – Fuel Storage

- Tank size determines running time
- Day tank or bulk tank?
- Local regulations may require double-bunded tanks

© CNet Training

Fuel storage is an issue to consider. Day tanks may be fitted to the generator, giving about eight hours running, or bulk tanks may be needed for longer periods.

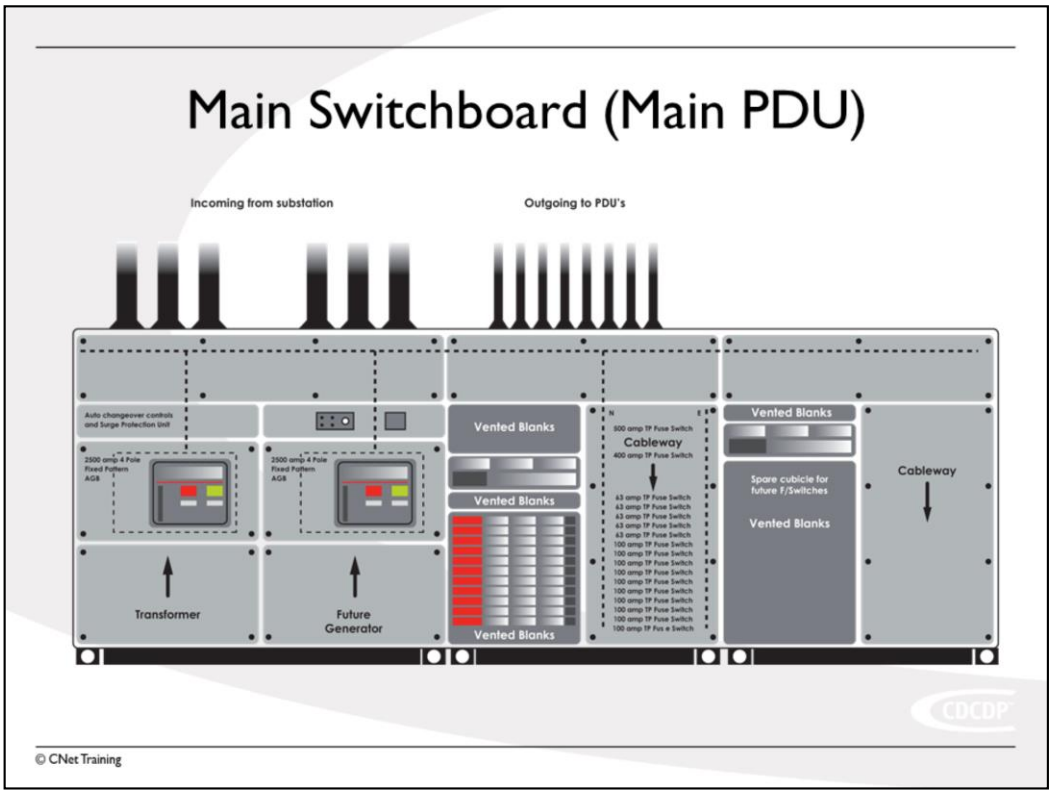
Health and safety commonly requires a double-bunded tank (tank within a tank) to capture any fuel spillage.



It is necessary to maintain fuel in good condition or it will deteriorate, and the generator may not start when required.

Instead of washing the oil, some Data Centres carry out a full system test and switch over to the generators every six months, using all fuel up. This may be viewed as 'brave' or 'sensible' depending on your viewpoint.

A well-designed and operated Data Centre may consider this option as it proves the standby power system will work when needed, but the carbon commitment may influence this.

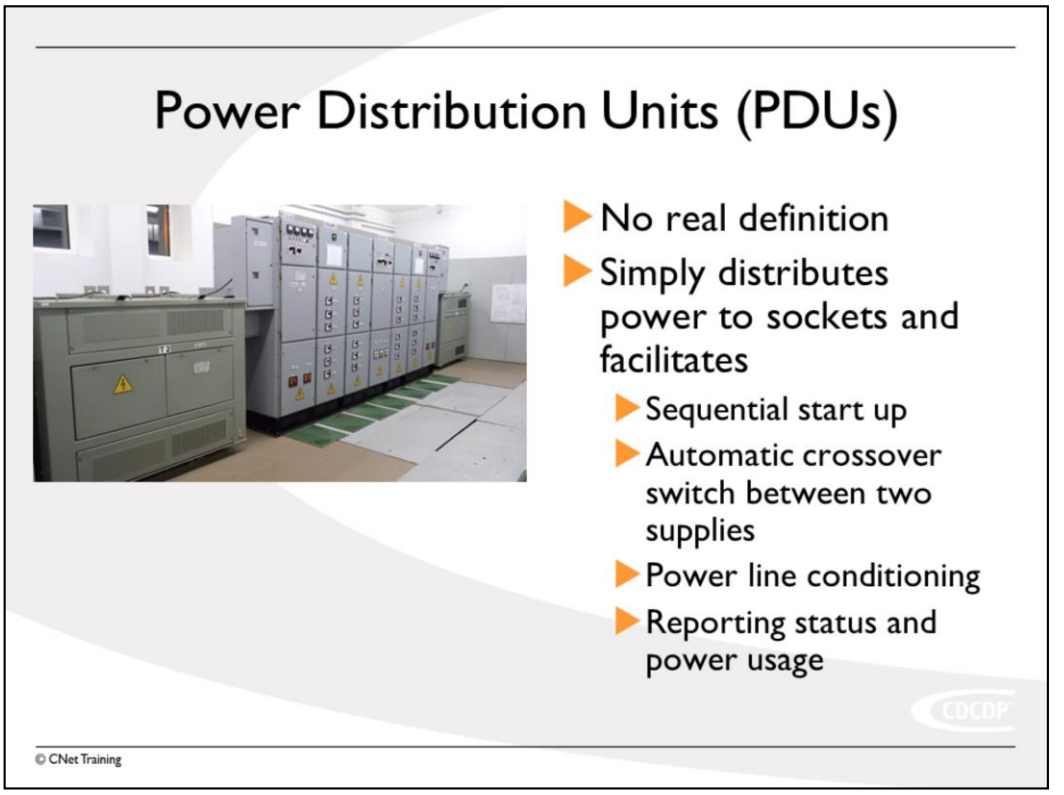


Electrical power is presented to the Data Centre through a switchboard (or switchboards), similar to the one shown.

The incoming circuits are split into a number of outgoing circuits to feed different areas or loads within the Data Centre. The outgoing cables are protected by an appropriate fuse or circuit breaker, such that a fault on any circuit will only affect that circuit and not trip out the entire facility.

The cables feeding loads may be single or three phase, and will also contain neutral and earth conductors.

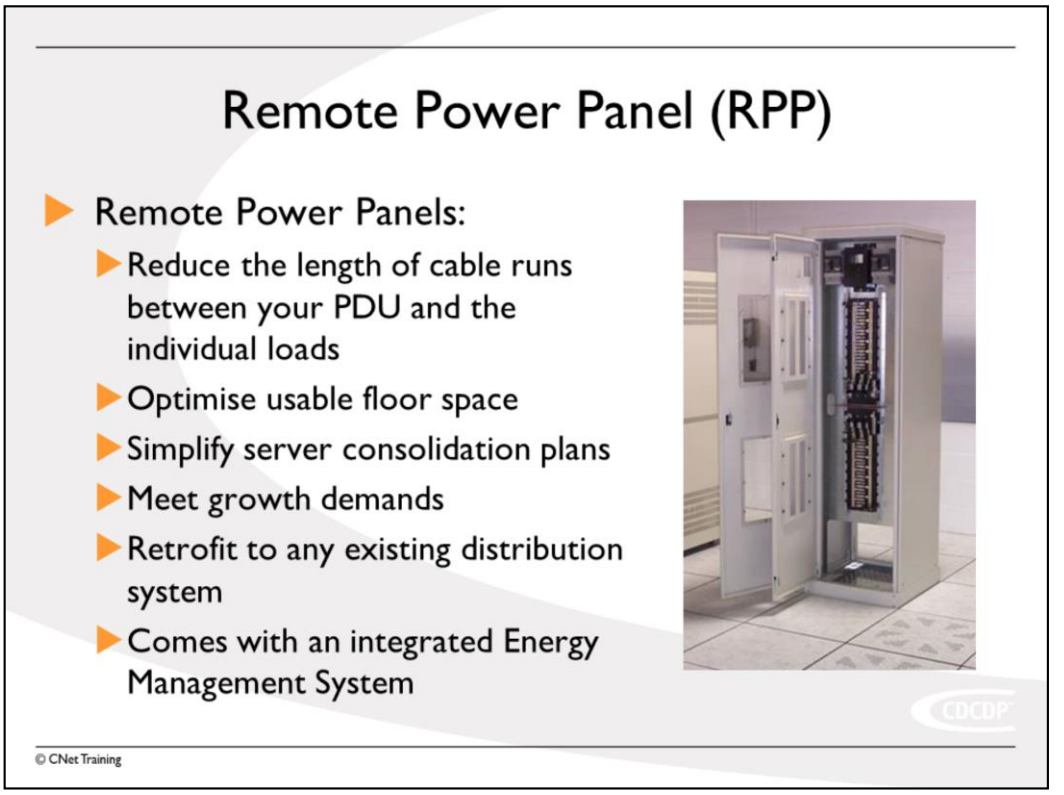
Note: The feeds from the utility provider are high voltage and low current, which allows them to utilise smaller conductors for greater distances. However, the Data Centre works on low voltage and higher current, which can result in larger conductors. This is a key factor the CDCD needs to appreciate when documenting the primary electrical components.



Once we get into the computer room, the power needs to be further distributed to individual pieces of equipment. This is achieved through power distribution units (PDUs) - in effect, a cut-down version of the main switchboard.

PDUs are not clearly defined by Standards and they come in many sizes, but they all have common features and functions.

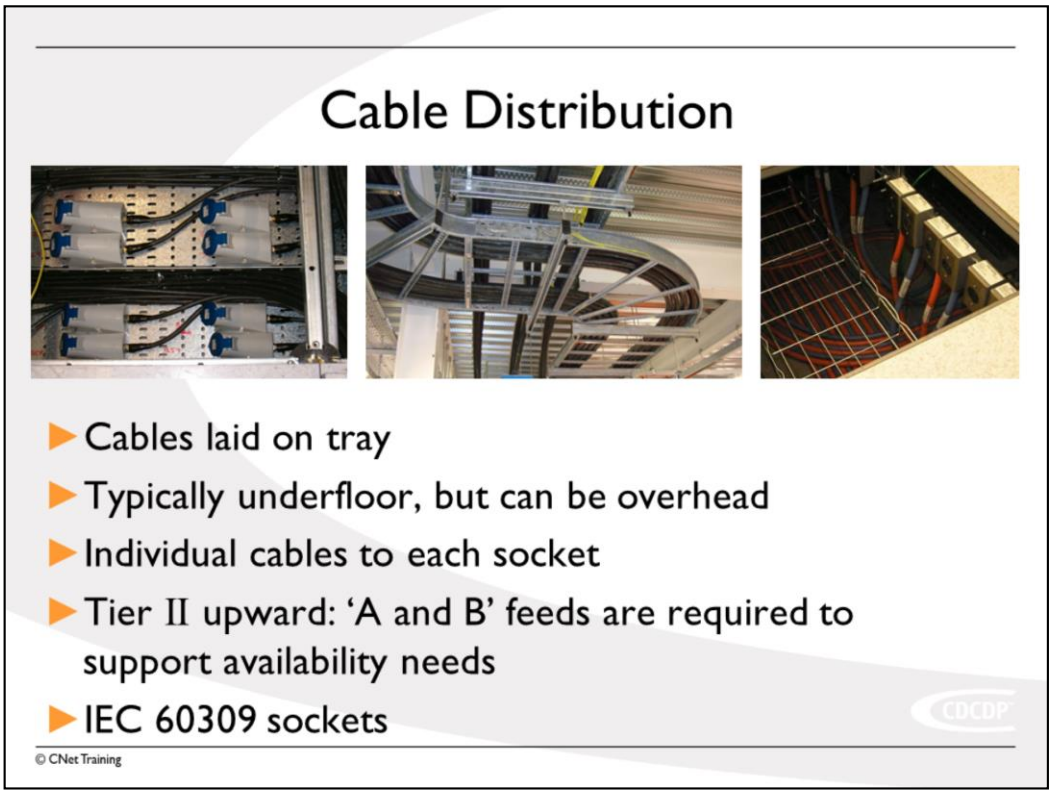
The basic function is to distribute power to the racks, either through cables and sockets, or via an overhead bus-track system.



The use of Remote Power Panels is now fairly common in the USA, and is becoming more common elsewhere. RPPs can have an impact on the size of the Final or Branch conductors, and therefore the energy losses in the cables. A Remote Power Panel offers a customisable, scalable solution for expanding your Data Centre power distribution efficiently and cost-effectively. One of the primary attractions of an RPP is increased distribution capacity in a compact design. The RPP can be placed at the end of a server rack aisle, or within an aisle to help reduce cable costs.

This feature decreases the length of cable runs between the RPP and your peripheral loads, eliminating clutter and further optimising the use of expensive Data Centre floor space. As a standalone unit, the RPP can be retrofitted to any existing distribution system, providing easy expansion of power distribution in your Data Centre. Moreover, it simplifies future expansion to meet increased load requirements for both single or dual-corded equipment.

RPPs are also equipped with an Energy Management System. The Energy Management System provides monitoring and alarming capabilities that allow the user to monitor power consumption and quality, manage and plan power needs, and react quickly to potential problems down to the branch circuit level.



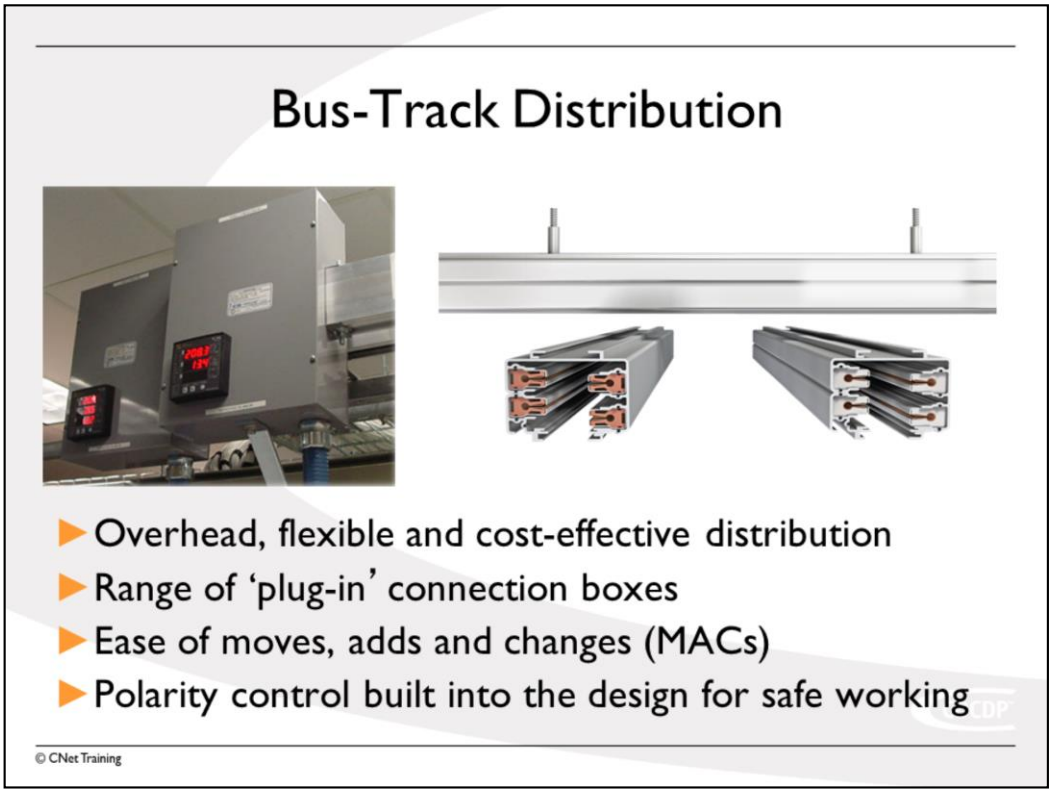
Power distribution to the racks in a computer room can be achieved using cables as shown.

Each socket position is fed by its own cable, which connects all the way back to the PDU. The IEC 60309 socket is specified in the Standards.

The overall cable installation will be subject to local codes and regulations, which will cover requirements such as:

- Cable size for current capacity and volt drop
- Separation distances from other services, including data cables
- Support requirements, such as traywork (heavy duty)

The CDCD must discuss these requirements with the electrical designer. From a Tier II Data Centre upward, an 'A' feed and 'B' feed are required to support availability needs, so dual provision of cable routes and switch gear is required.



Bus-track electrical distribution can also be used. This is not new, and has been used for many years.

It is a simple and versatile solution for supplying power to electrical loads; the busway can be quickly tapped at any location, with a variety of plug-in units, to allow for fast MACs in a Data Centre.

The busways generally have some form of polarising method to prevent mismatched components from being inadvertently connected to each other, preventing cross-phasing during installation. Not all systems are compatible, so the CDCD needs to be aware of this.

Power to the Rack

- Single phase (usually) to the rack
- Two feeds for redundancy
- 16A, 3.6kVA
- 32A, 7.2kVA
- 3-phase for more power
- IEC 60309 connectors
- National and local variations are present

	North Amercian	International
Yellow	125V	100-130V
Blue	250V	200-250V
Red	400V	380-480V

© CNet Training

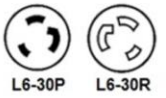
Power to equipment racks is normally single phase via IEC 60309 connectors.

It is typical to provide two feeds to each rack from difverse PDUs.

It is becoming more common, particularly in server racks, to provide a 3-phase supply in order to meet increased power demands. Three-phase supplies must be positively identified.

Power to the Rack – US Variations

Size / type	Straight-blade connector	Twist-lock connector	Comments
208 Volt 15 Amp	NEMA 6-15P	NEMA L6-15P	2496 VA equipment load
208 Volt 20 Amp	NEMA 6-20P	NEMA L6-20P	3328 VA equipment load
208 Volt 30 Amp	None	NEMA L6-30P	4992 VA equipment load
125 Volt 3-phase 30 Amp	None	NEMA L14-30P	8640 VA equipment load



- There are a number of options utilised in the US

Source: APC Schneider

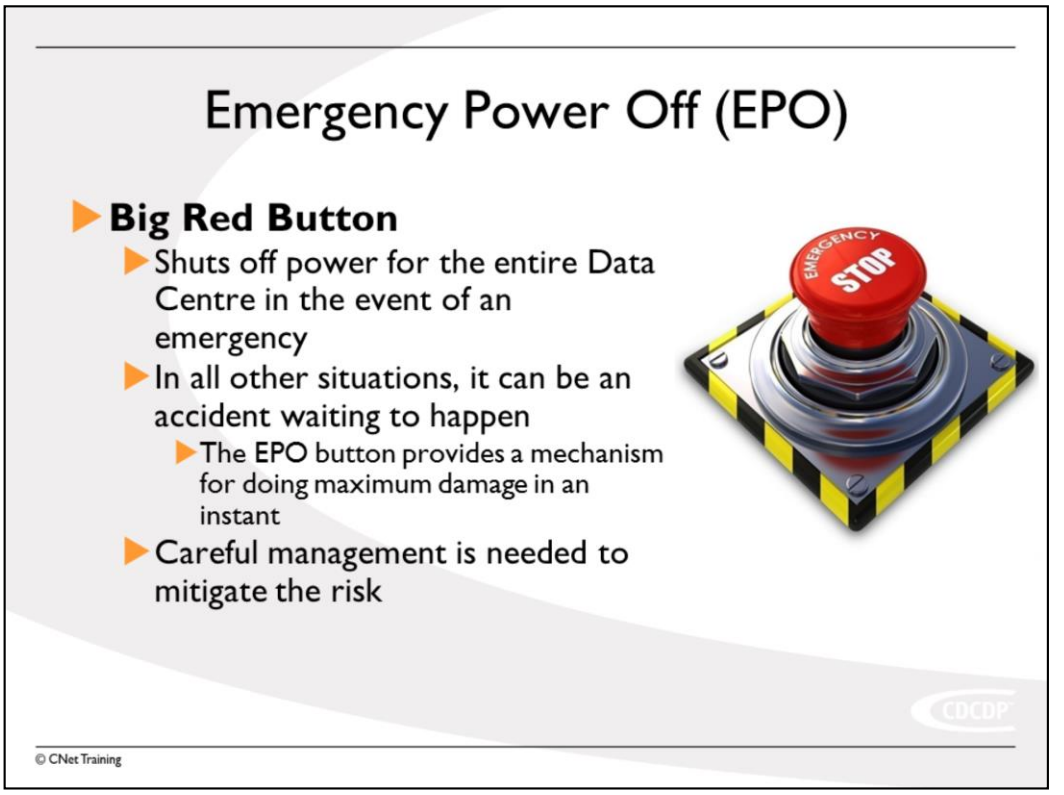
© CNet Training

Power in the Rack

- A wide range of options available
- Single phase and 3-phase
- Horizontal or vertical
- Metered or unmetered
- IP addressable
- NEMA or IEC style outlets and plugs
- Available with thermal circuit breaker to protect circuits from overload
- Optional surge protection to protect equipment from power spikes
- Optional local current meters to provide easy load monitoring

© CNet Training

Power to equipment within the rack is provided by distribution strips. There is an ever-increasing range of options to choose from. Some of these are simply connector blocks, while some have inbuilt 'intelligence', are IP-addressable, and feature additional circuit protection. The CDCD should establish the most appropriate for the application.



Once we have provided secure power to the critical IT load (so it remains on at all times and under all eventualities), we surely need a simple way to undo all that effort in one fell swoop, putting in a manual trip button, don't we?

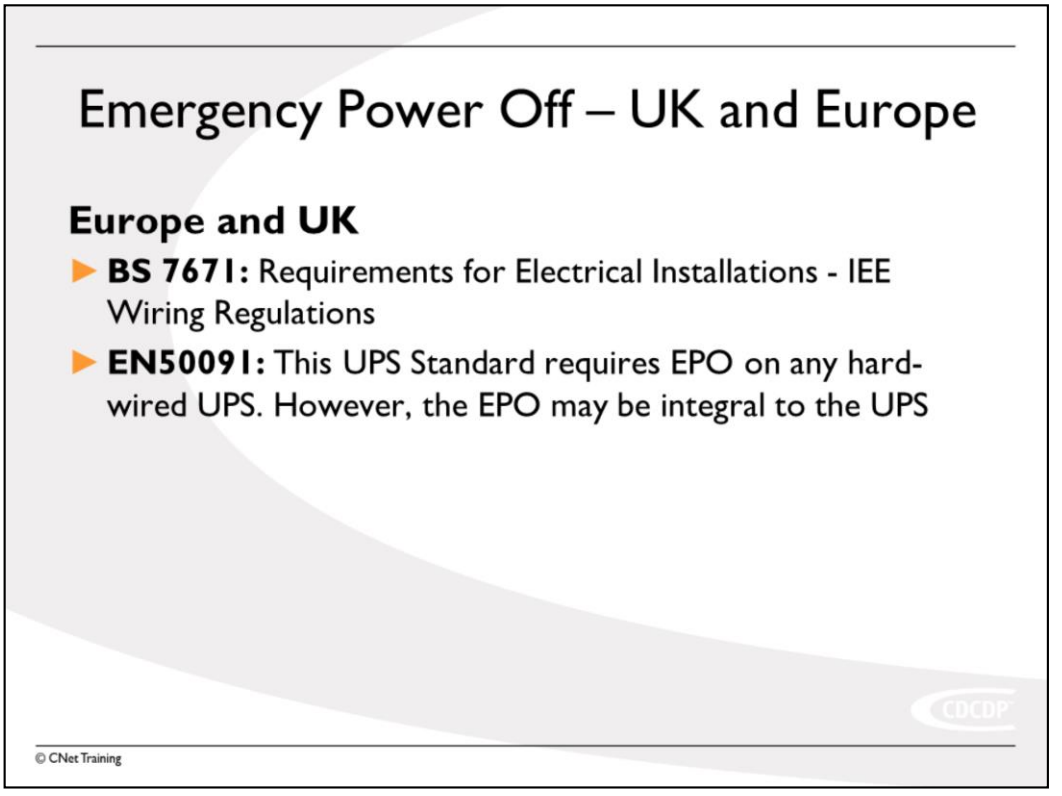
There are lots of stories about the EPO button in Data Centres, and few of them have happy endings.

EPOs present one of the greatest risks to electrical system uptime in the Data Centre.

Accidental EPO activations occur via employee sabotage, accidental activation and routine maintenance.

Regulations call for a single point of shutdown on 'certain electrical installations'. This is difficult to achieve in a Data Centre, and current thinking varies between designing very complex systems to claiming Data Centres are not included in 'certain electrical installations'.

One school of thought is that EPOs should be eliminated in Data Centres. High level discussions continue, particularly in the USA, and the CDCD needs to be aware how this issue develops.



There are no statutory requirements in the European regulations for emergency stop in Data Centres.

Emergency Power Off - USA

- Emergency power off functions are included in the NFPA 75 Standard
- The Standard calls for a means to disconnect:
  - Power to IT equipment (PDU)
  - Power to HVAC systems
  - Power to the UPS, if located in the computer room
- This can be achieved by separate controls
- How can we prevent unintentional EPO operation?
  - Cover it and make it difficult to operate? (Some options include high-decibel alarms)
  - Monitor it with CCTV?
- Local fire codes do not always mirror the Standard

© CNet Training

The Standard calls for a means to disconnect power to all electronic equipment and dedicated HVAC systems. These functions don't have to be governed by a single mechanism, and there is the option of separate buttons to terminate the IT equipment power as well as HVAC systems.

The Standard says shut-off systems must be 'grouped, identified and readily accessible' and located at the main exit doors.

One recommendation is to use three EPO buttons:

- PDUs
- HVAC units
- UPS feed to the Data Centre

If the UPS units are in an equipment room separate from the Data Centre, they do not need to be controlled by the EPO.

Richard Sawyer of EYP Mission-Critical Facilities, says 'Cover it and make activation a positive, intentional, multi-step action. Make sure signs are posted in the language spoken by the cleaning crew. Put an alarm on the cover. You need to make them stop and ask themselves: Do I really like my job? Is this a good career move?'

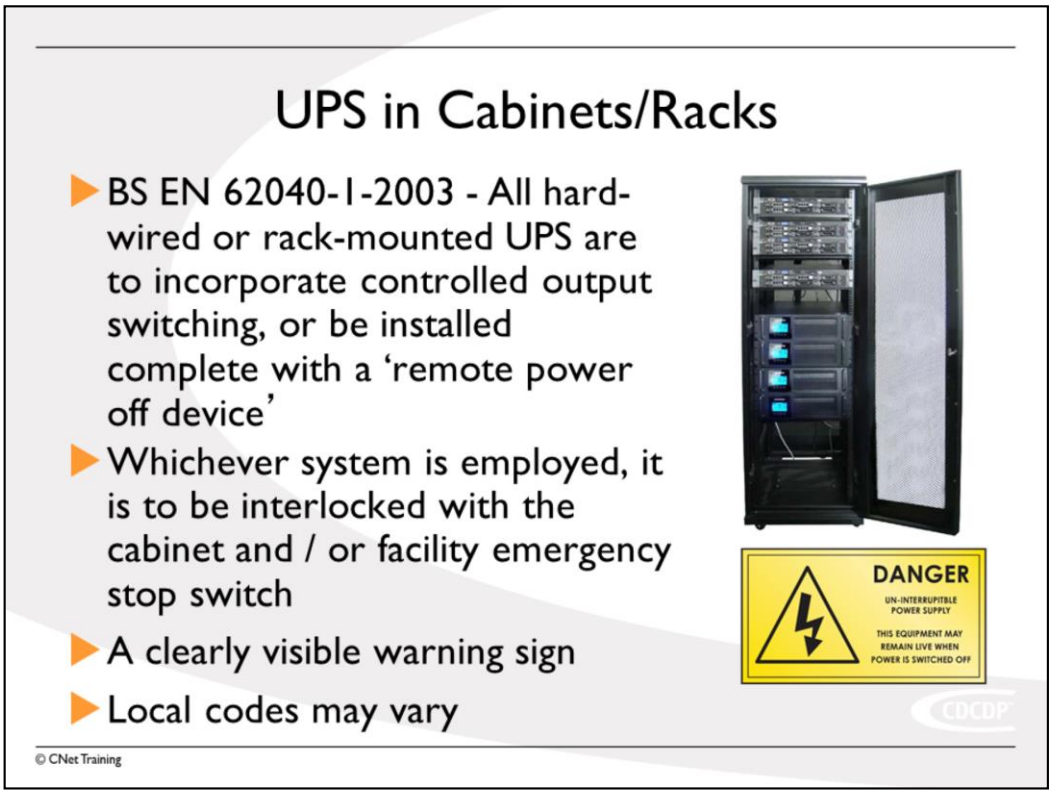
Sawyer also advocates monitoring the area with video cameras to deter sabotage.

Managing the EPO

- EPO should:
  - Be a three-stage system, with off, test and armed modes of operation
  - Require three steps to operate (such as lift, hold and pull), or require the simultaneous operation of two or more buttons
  - Offer a pre-alarm function, such as an audible and visible alarm when a button cover is lifted
  - Be on a time delay, if allowed by local jurisdiction
  - Be monitored by CCTV
  - Not be located near light switches, phones or any other device that is routinely touched
  - Be isolated from the fire alarm system to prevent accidental activation

© CNet Training

If an EPO is necessary, the designer should include some of the above 'best practices' to minimise the risk of false operation.



Irrespective of the requirement for an EPO which disconnects the entire Data Centre, EPO look-alikes may be required for certain elements within the Data Centre.

Rack-mounted UPS systems have their own requirements for disconnecting outputs, either locally or remotely, to enable safe working on equipment in racks.

If an EPO is installed, there should be an interlock to ensure the rack UPS outputs disconnect when the EPO is activated, such as a remote means of operation (also known as a Remote EPO or "REPO").

Equipment supplied by a UPS should be clearly identified, as in the sign shown. This particularly applies to the IT equipment racks in a Data Centre.

Estimating Power Requirements

- Typical assumptions
  - Nameplate values are generally derated by 33% for normal running power
  - UPS efficiency typically 88%
  - Recharging UPS batteries need 20% of rated power
  - Lighting: Allow 21.5W per m^2
  - Air conditioning can take as much as 100% of its rated cooling capacity
- These estimations are the initial 'ballpark' figure, which then needs to be analysed and refined to provide a more accurate understanding of the power requirement

© CNet Training

There are some rules of thumb that enable the CDCD to estimate the size of the incoming supply required by the Data Centre. At this stage, you can calculate power requirements for the computer room by completing an estimation sheet through a series of designated steps. Without getting too deep into the complexities of the electrical design, the CDCD can use this to give a sensible ballpark figure, which can be refined when better information about the actual Data Centre equipment is available.

Estimating Power Requirements (Basic Example)

Nameplate rating of I.T. devices x 0.67	kW (1)
Rating of other devices x 0.67	kW (2)
Future expansion loads	kW (3)
Subtotal, running load 1+2+3	kW (4)
Add 5% for peak load factor (4) x 0.05	kW (5)
Add 32% to running load for UPS inefficiency and battery charging (4) x 0.32	kW (6)
Lighting, 0.0215kW x floor area in sq. m	kW (7)
Total power demands (4+5+6+7)	kW (8)
Add power for cooling, 1 x (8)	kW (9)
Total with overrating factor of 1.25 ((8) +(9)) x 1.25	**kW (10)**
Current capacity = (10)/input voltage	A (11)
Generator capacity = (10) x 1.03* *PF correction	kVA (12)

© CNet Training

There are many different calculators around and the designer can choose one he/she prefers. This checklist is a simple method which will give a 'safe' answer but, if better information exists about equipment efficiencies etc., then it should be used to refine the calculation.

Review

- Can you?
  - Understand applicable regulations and codes
  - Identify where power is used
  - Identify the key power components
  - Discuss power distribution options
  - Discuss emergency power off (EPO)

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 4

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

Cooling

Version 1509

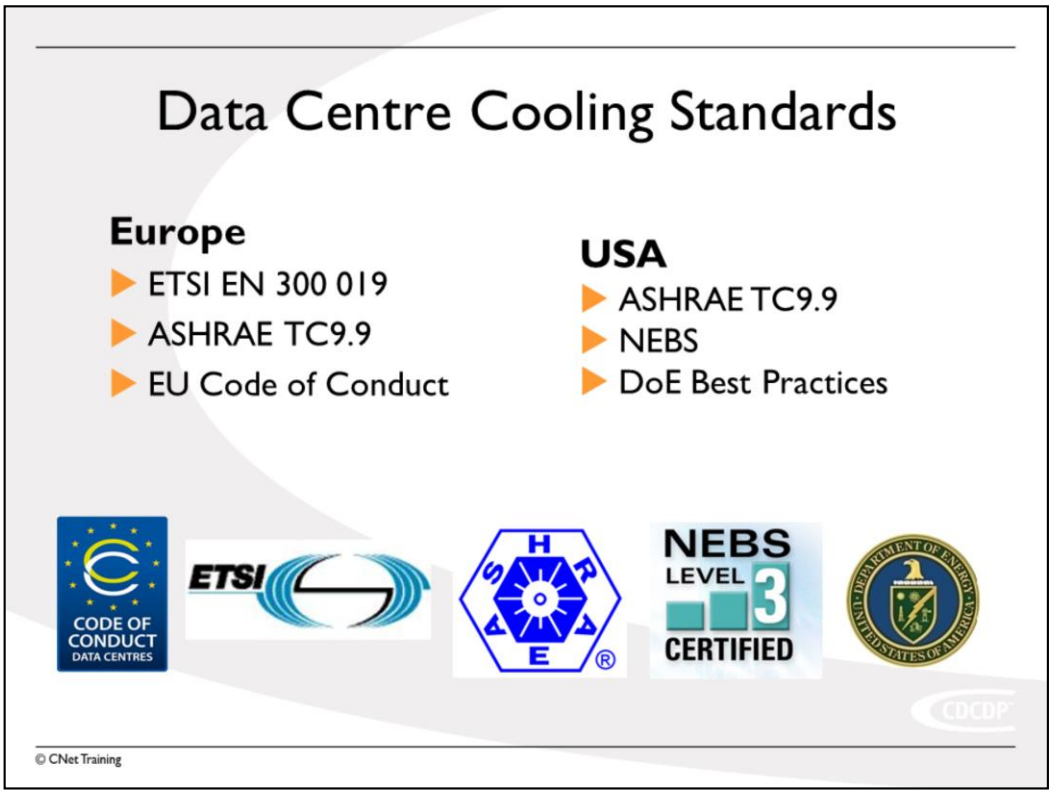
CDCDP

Objectives

- At the end of this module you will be able to:
  - Understand the applicable Standards
  - Understand the primary purpose of cooling
  - Identify the key cooling components
  - Discuss cooling options

CDCDP

© CNet Training



Since other industries may be involved in the Data Centre design, the designer should also be knowledgeable about the related Standards, local regulations and national regulations appropriate to the region.

Worldwide

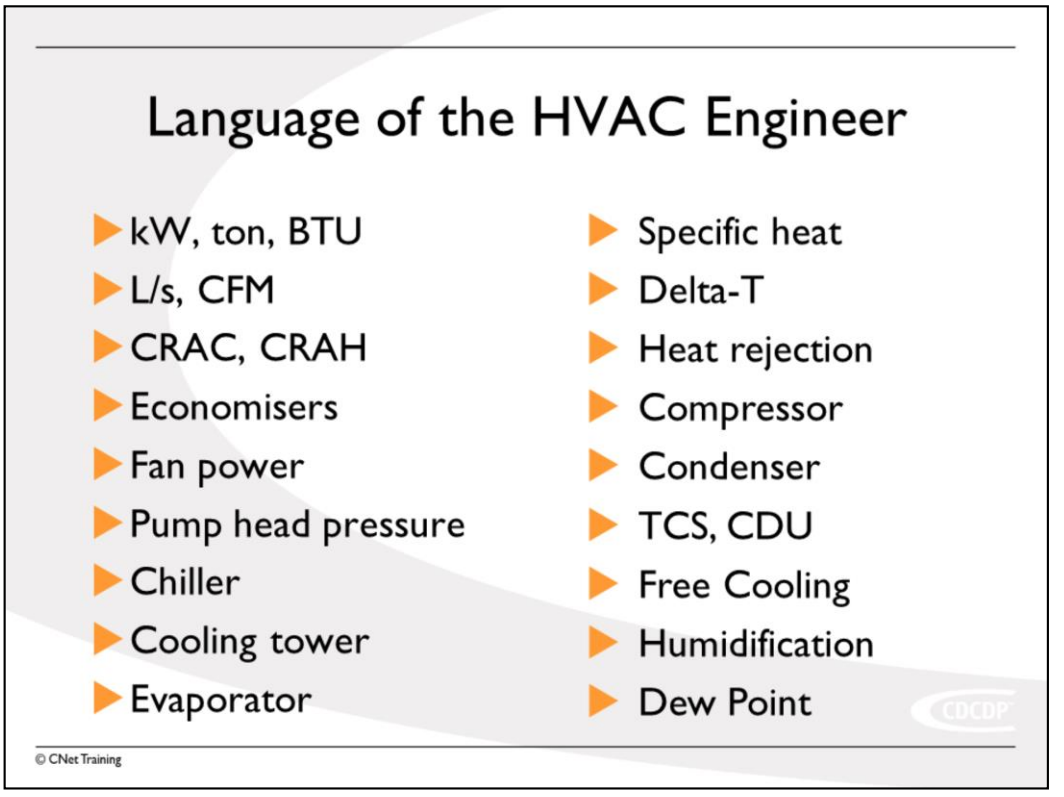
- On a worldwide basis the USA or EN Standards are used

USA

- American Society of Heating, Refrigeration and, Air-Conditioning Engineers (ASHRAE) tends to take the lead in the USA with the telcos working to the Telcordia Network Equipment Building System (NEBS) Standard. The Department of Energy Data Centre Energy Productivity (DCEP) programme has produced a list of best practices which are very similar to the EU Code.

Europe

- Europe follows European Telecommunication Standards Institute (ETSI) and ASHRAE recommendations, and the EU Code of Conduct builds on these in its Best Practice Guide



The CDCD needs to be able to understand the engineering language used by HVAC engineers so that he/she can have a meaningful discussion with them.

We are not covering this in great detail here as it is covered in more detail during the CDCDP course.

- CRAH – Computer room air handling unit
- CRAC – Computer room air conditioner
- TCS – Technology cooling system
- CDU – Coolant distribution unit

The Primary Purpose of Cooling

- IT equipment consumes electricity and leaves behind heat as its ***"waste product"***
- The Data Centre is an enclosed facility - if not given an outlet, heat can build, damage, or destroy servers and other electronic devices
- The primary purpose of cooling is to remove heat from the Data Centre
- The CDCD must fully evaluate the potential IT load to ensure appropriate cooling capability is designed to effectively remove the generated heat

CDCDP

© CNet Training

Data Centre heat removal is one of the most essential yet least understood of all critical IT environment processes. As the latest computing equipment becomes smaller and uses the same or even more electricity than the equipment it replaced, more heat is being generated in Data Centres.

The goal of Data Centre cooling is to move heat from the indoor environment (the Data Centre) to the outside, and to maintain a temperature conducive to proper functioning (and, preferably, long life) of servers and other equipment.

Precision cooling and heat rejection equipment is used to collect and transport this unwanted heat energy to the outside atmosphere.

What is Important to Data Centre Operations?

- Performance - Heat loads that do not go away
- Efficiency - Controlling costs
  - Capital Expenditure (CAPEX)
  - Operational Expenditure (OPEX)
- Reliability - Availability is critical
- Flexibility – Long-term planning
- Service - Controlling costs
  - Maintenance
  - Procurement

© CNet Training

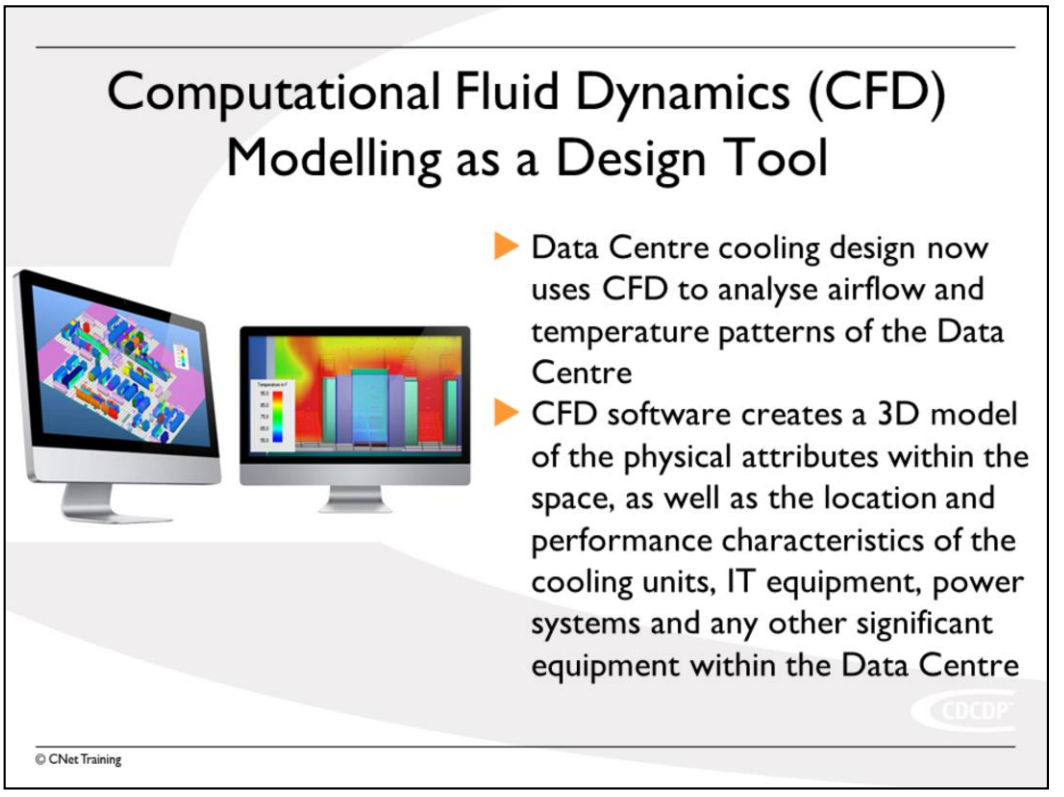
Cooling Continuity Plan

- The CDCD needs to work with the HVAC Engineer to formulate a detailed Cooling Continuity Plan (CCP) to ensure the cooling supply is maintained to the IT critical load under all applicable situations
- The Data Centre must have a plan to ensure heat removal from IT critical loads is maintained
- This will document how the HVAC plant should operate under all conceivable situations
- It will cover all component parts of the HVAC protecting the IT equipment

© CNet Training

A Cooling Continuity Plan (CCP) should be prepared by the CDCD together with his/her HVAC engineer. The CDCD needs to provide key design information, such as:

- Projected cabinet load (kW)
- Raised access floor or slab construction floor design
- Depth of access raised floor (if applicable)
- Position of cable containment systems (underfloor or overhead)
- Monolithic (fully demand) or modular based design
- Specialist environmental demands
- Architectural factors (pillars and alcoves)

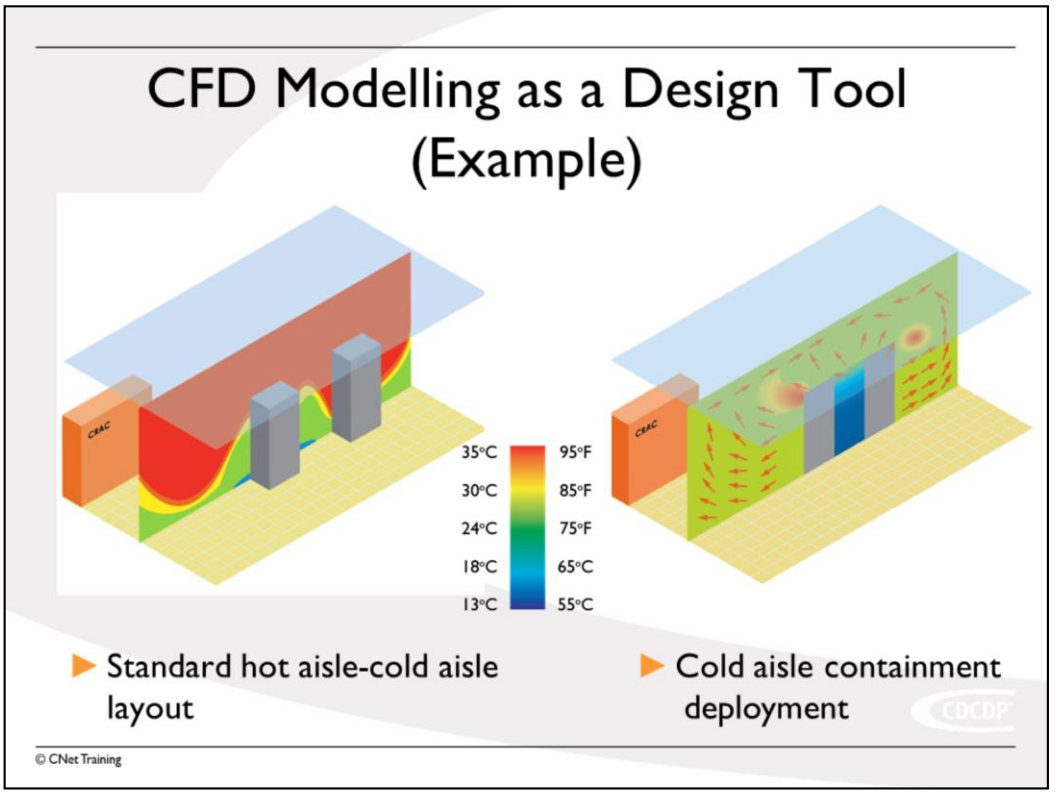


The CFD provides a complete and detailed thermal understanding of the Data Centre. This involves the CDCD proving data pertaining to:

- Physical layout of the space and equipment in the Data Centre.
- Data Centre power equipment thermal dissipation and rack power density.
- Environmental conditions.
- Cooling capacity and utilisation and air distribution effectiveness.

A 3D CFD model of the Data Centre is created based on the information collected onsite.

- The CFD can provide an analysis of a baseline model, an optimised model, and a maximised model, which simulates site recommendations.



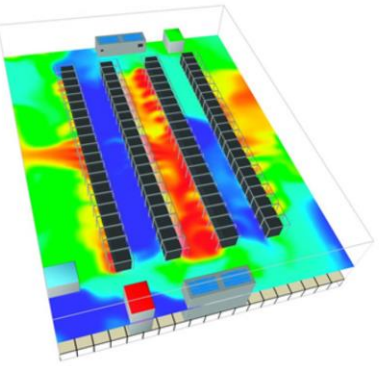
CFDs can analyse the proposed airflow within your Data Centre and provides a graphic illustrated analysis of how hot and cool air flows, which is proving essential to gain the most efficient design. Here are two such examples:

- The temperature distribution in a standard hot aisle-cold aisle model demonstrates the temperature rising significantly towards the top of the racks
- The temperature distribution in a cold aisle containment model demonstrates that there is a minimal difference in temperature between the bottom and top of the racks

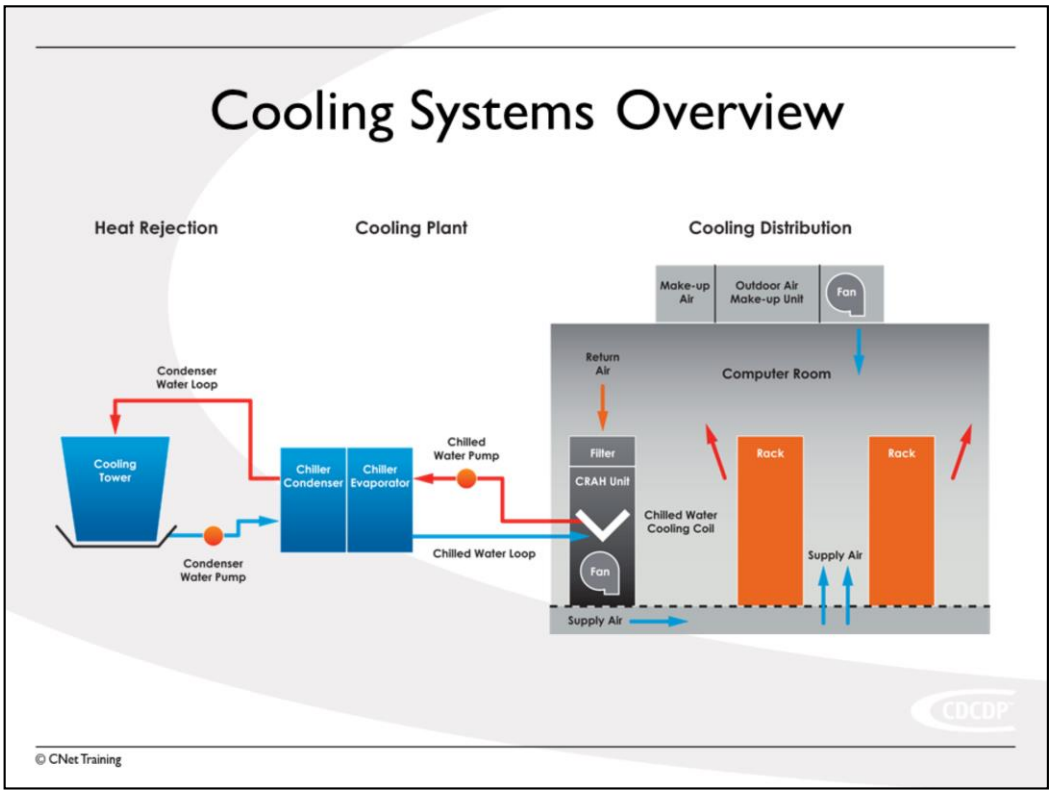
This capability minimises the need to rework the cooling supply and return air temperature paths, which can be a costly affair impacting upon completion timeframes

CFD Design Benefits

- CFDs provide key benefits:
  - Assesses the performance of existing facility layout
  - Validates proposed design, ensuring it will operate as efficiently and reliably as possible
  - Makes accurate predictions at all stages of the cooling design process
  - Provides the ability to assess the precise temperature and airflow modelling to correctly support the Data Centre
  - Provides a cost-effective and energy efficient design



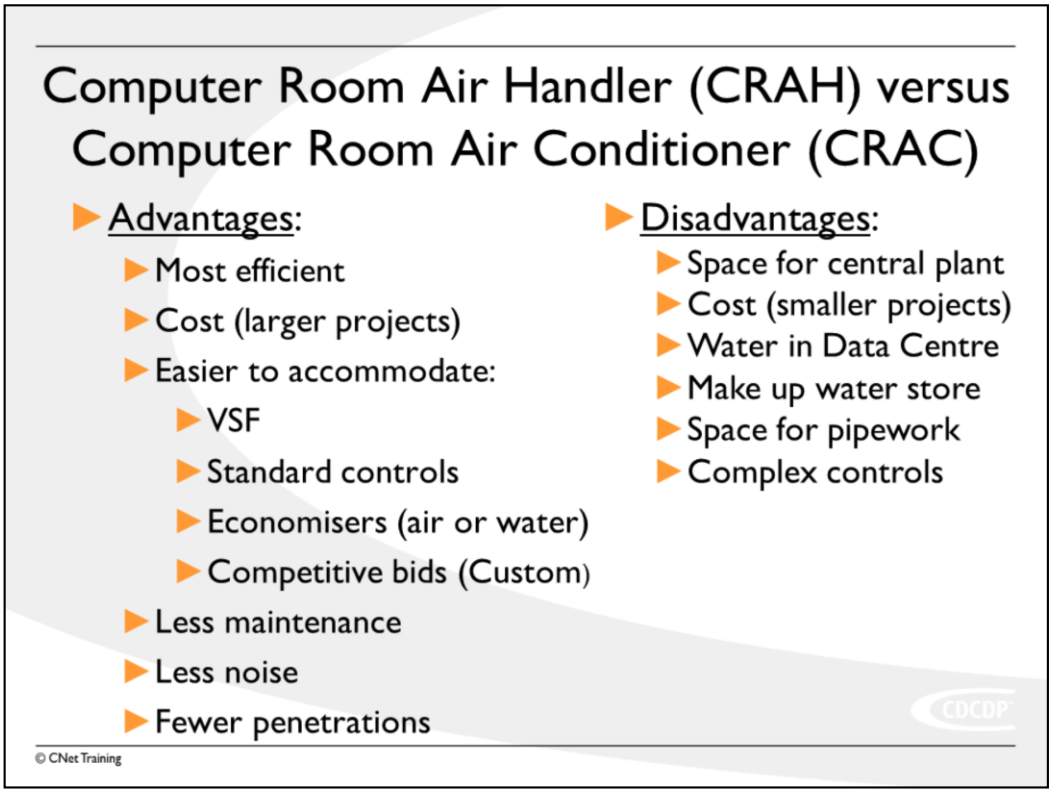
© CNet Training



Air conditioning, as a basic principle, is simple:

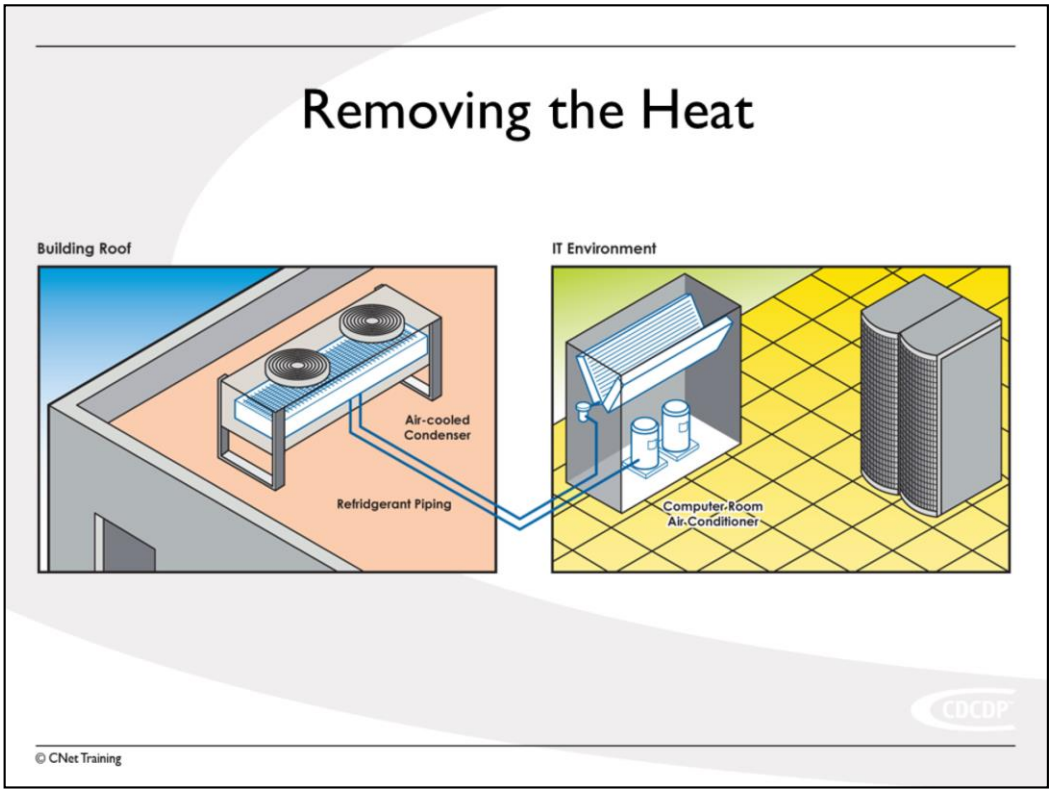
- Heat is generated by equipment inside a room
- The air conditioning system removes the heat and dumps it outside

The cooling system should be able to remove all the heat generated by the IT load, but its efficiency decreases at partial loads. There may be just one, or there may be several stages in the cooling system.



CRAH and CRACs, although they perform a similar function, are fundamentally different in many respects. As a result, they each have pros and cons depending on the application.

- **CRAC** - Computer Room Air Conditioner has an internal compressor and utilises direct expansion of refrigerant to remove heat.
- **CRAH** - Computer Room Air Handler has fans and cooling coils, and uses chilled water to remove heat.



Inside the computer room, air is used in the majority of Data Centres to transfer heat from the IT equipment to the CRAC or CRAH. There is a need to control the environment within the room accordingly.

One of the key purposes of the Data Centre is to provide an environment where IT equipment will perform reliably and within given parameters - it is important to know what that environment should be.

ASHRAE Operational Parameters 2011

ASHRAE 2011 Equipment Environmental Specifications					
Classes	Product Operation				
	Dry-bulb temperature (°C)	Humidity range non-condensing	Maximum dew point (°C)	Maximum elevation (m)	Maximum rate of change (°C/hr)
Recommended					
A1 to A4	18 to 27	5.5°C DP to 60% RH and 15°C DP			
Allowable					
A1	15 to 32	20 to 80% RH	17	3040	5/20
A2	10 to 35	20 to 80% RH	21	3040	5/20
A3	5 to 40	8 to 85% RH	24	3040	5/20
A4	5 to 45	8 to 90% RH	24	3040	5/20
B	5 to 35	8 to 85% RH	28	3040	N/A
C	5 to 40	8 to 85% RH	28	3040	N/A

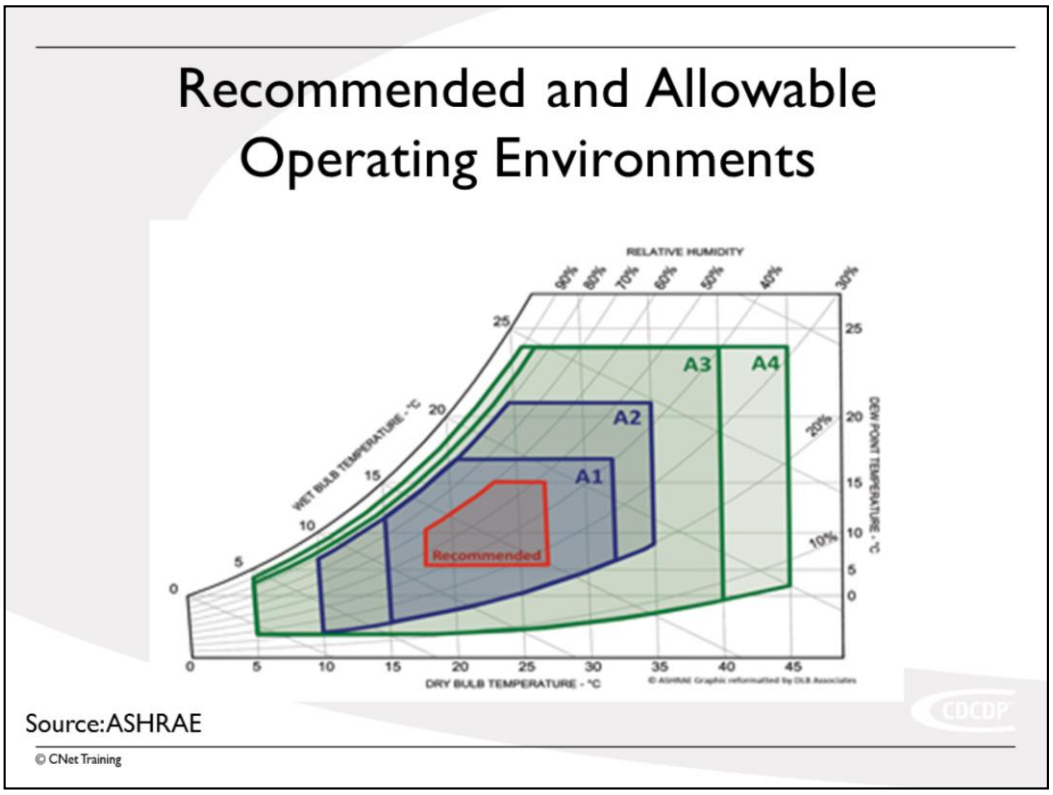
Source: ASHRAE

© CNet Training

ASHRAE Standards had until recently recommended very tight parameters within the computer room. Some of these parameters have been extended as better knowledge of Data Centres has been gained. They are now aligned with the NEBS/ETSI recommendations.

The key, however, remains with operators being able to accurately understand the correct operating parameters to support their equipment ranges.

- Recommended 18-27° C = 64-81° F
- A1 Class 15-32° C = 59-90° F
- A2 Class 10-35° C = 50-95° F
- A3 Class 05-40° C = 41-104° F



Recommended:

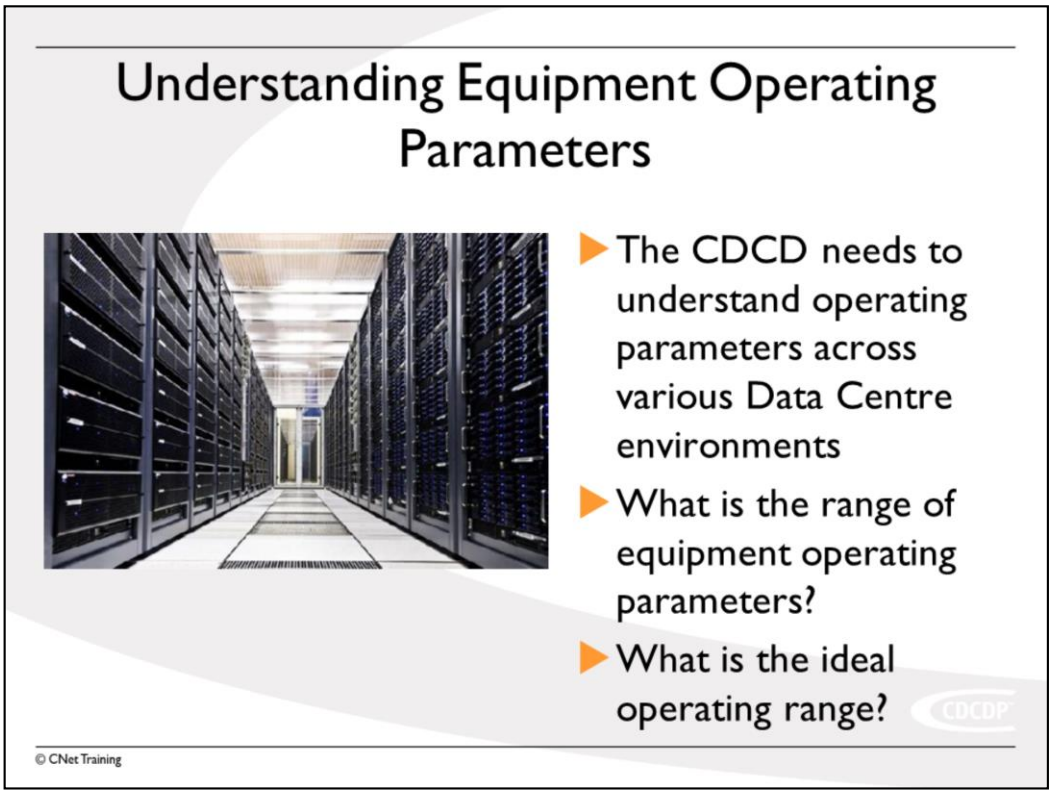
- Statement of 'reliability'
- Most equipment should be within this range, but short excursions into the allowable range are acceptable

Allowable:

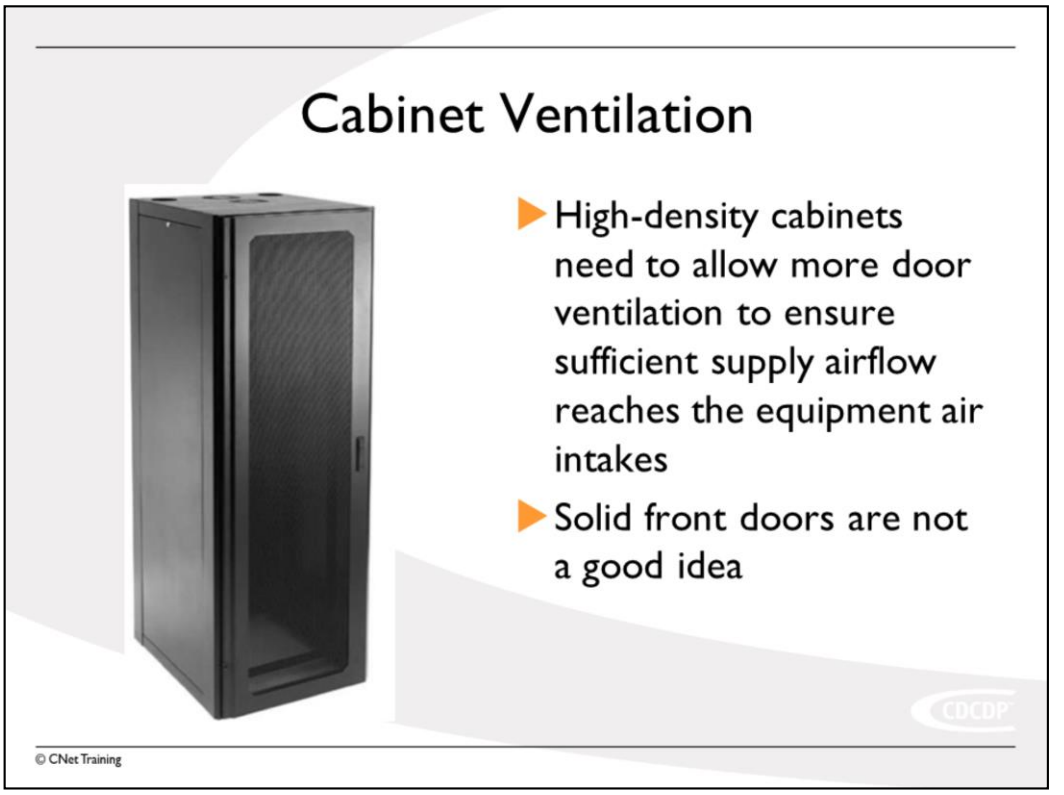
- Statement of 'functionality'
- No equipment should be outside this range

Manufacturers are now providing equipment capable of operating effectively within the A1 and A2 ranges. This is coupled with the likes of the European Code of Conduct for Data Centres, the US Data Center Energy Practitioner (DCEP) and other industry bodies encouraging Data Centre operators to utilise these higher operating parameters; the rationale behind the increased operating range has introduced a number of significant benefits:

- Reduces cooling burden
- Reduces humidifier burden
- Reduces carbon emissions
- Extends the operating lifecycle of the CRAC/CRAH



The importance of understanding the range of IT equipment operating parameters is essential to accurately maximise both cooling capability and effectiveness. Keeping environmental settings in the lower ranges of ASHRAE recommendations may be the safe option for many Data Centres, but it requires more energy and places more demands upon the operating capability of the cooling system.



As the operating environment for the IT equipment is that which appears at the air intake, the enclosure the IT equipment is mounted in can have a significant impact.

Older cabinets had solid or glass doors. These are not suitable for equipment cabinets that generate lots of heat.

High power cabinets (e.g., server cabinets) need to allow open ventilation to the front of the equipment, and so should either have no front door at all, or a highly-vented door to allow good airflow through the equipment. Solid doors should be replaced or removed.

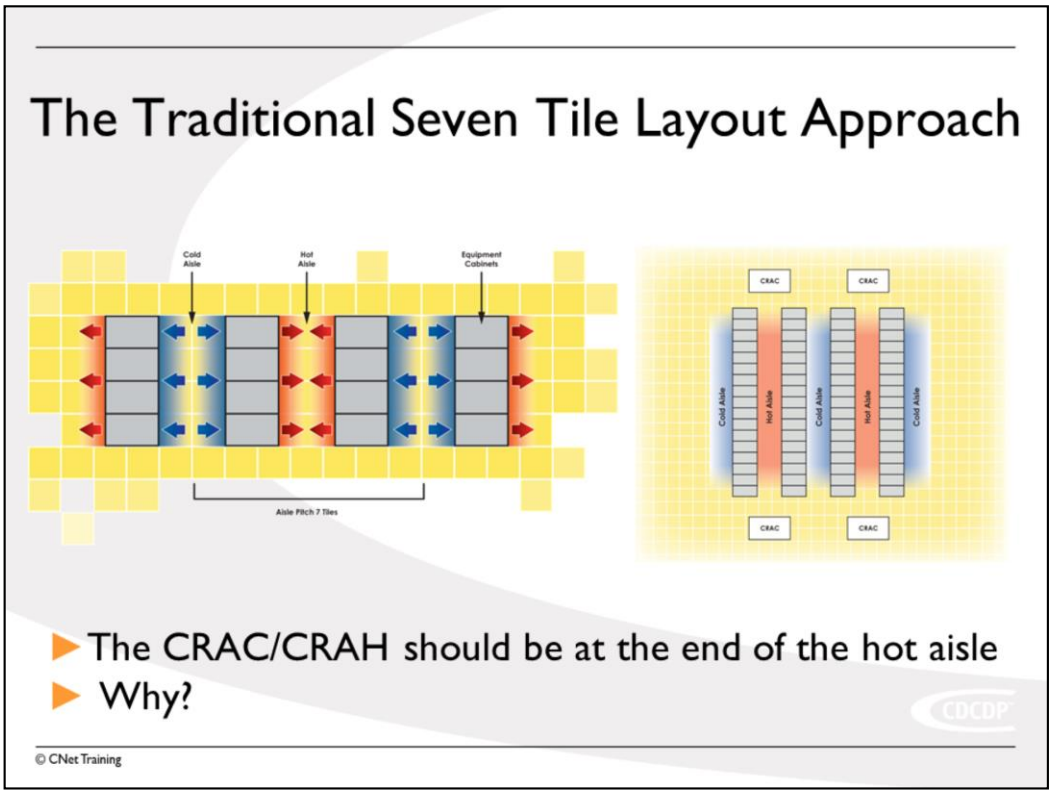
Arranging Cabinets in Aisles

- The EU Code of Conduct Best Practice Guide, TIA 942-A, BICSI 002 and ASHRAE, amongst many others, recommend laying out equipment cabinets according to the hot aisle-cold aisle model

© CNet Training

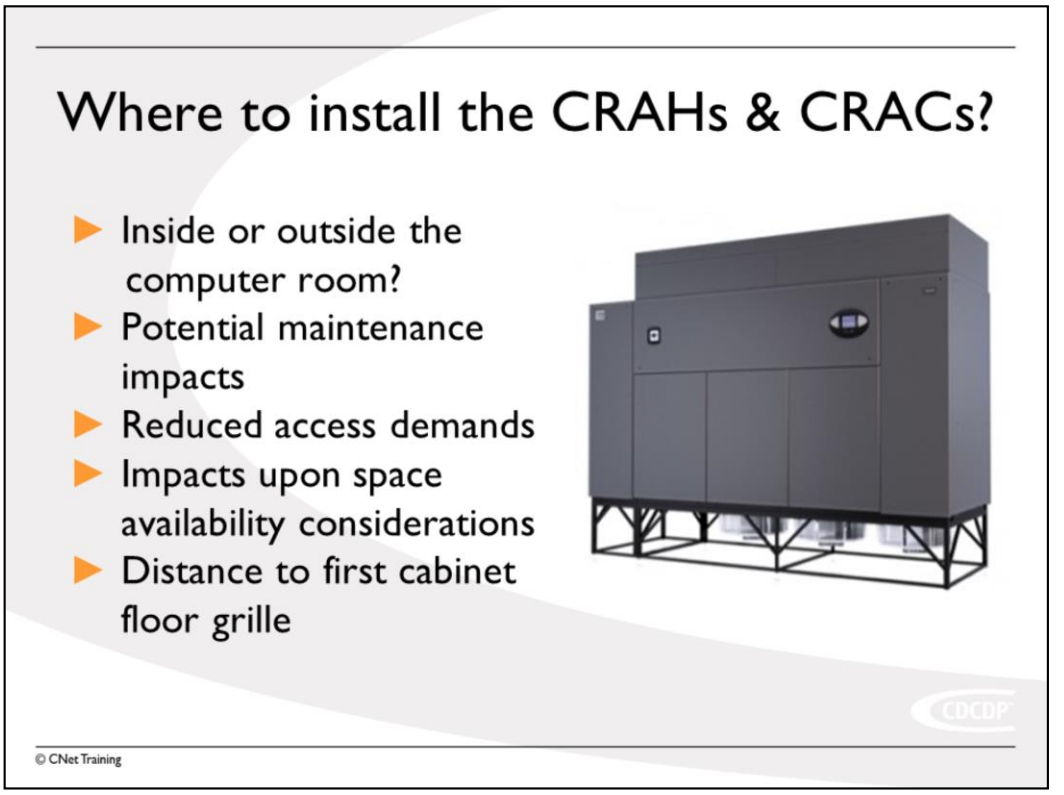
The common starting point for designing a cabinet layout in a computer room is to use the hot aisle-cold aisle model.

The model lays out the cabinets in a formation that repeats itself every seven tiles.



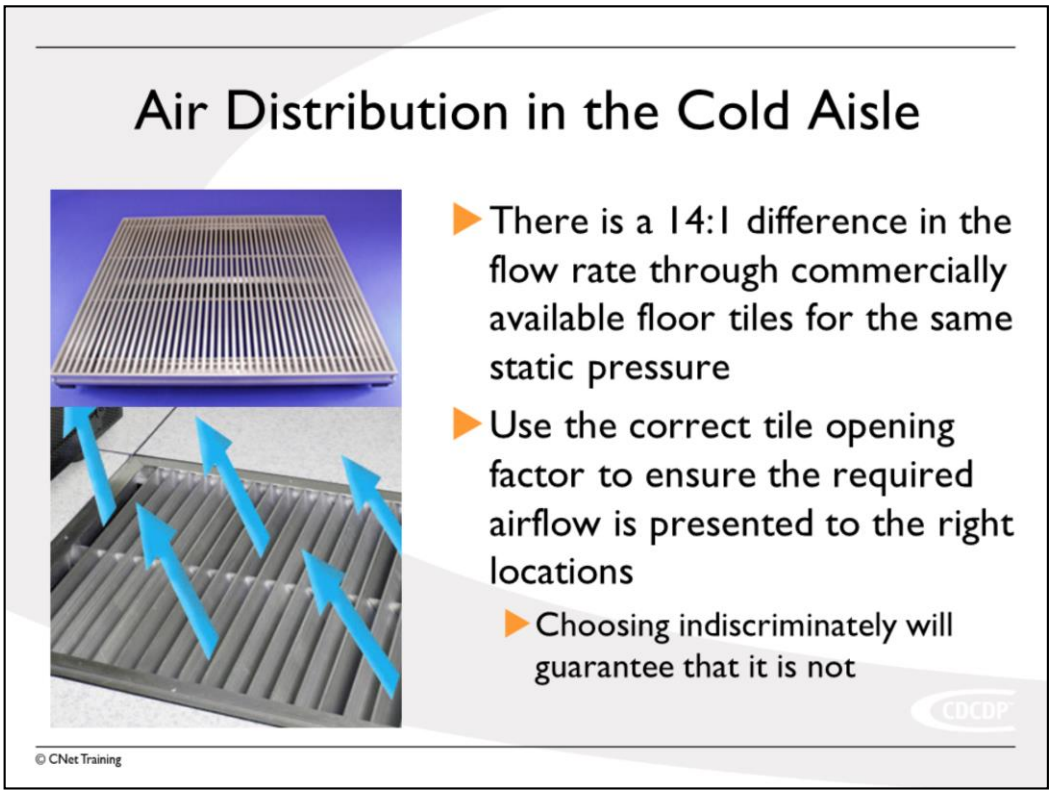
In the traditional seven tile hot aisle-cold aisle model:

- The hot sides of adjacent rows face towards each other to create the hot aisle and similarly, the cold sides create the cold aisle.
- Air conditioning units pump cold air into the floor void.
- Vents in the floor deliver cold air to the front of two lines of equipment cabinets facing each other – the cold aisle.
- Hot air escapes through the back of the cabinet into the hot aisle, where it returns to the air conditioning unit.



The positioning of the CRAH and CRAC units have a number of key design considerations that need to be assessed. Inside or outside the computer room is now a question being asked by designers. Traditionally, the CRAC and CRAH units have been installed on the inner computer room walls, but now designers are starting to install them against external walls (in corridors or dedicated rooms). This has introduced some good benefits:

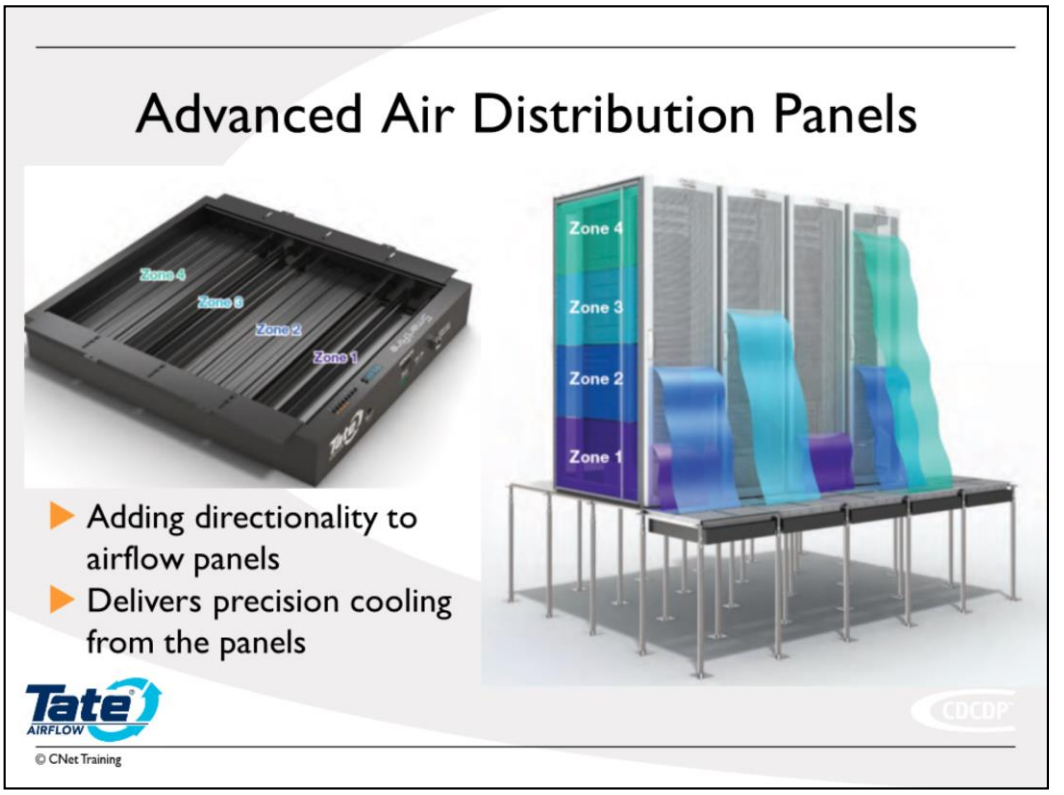
- Potential increased space within the computer room
- Easier maintenance access and reduced need to lift raised floor tiles
- Reduced computer room access requirements, especially third-party contractors



Air is commonly presented to the front of equipment racks through ventilated floor tiles. Not all ventilated floor tiles are the same! It is important to use the correct opening factor for tiles to meet the requirement. A one size fits all approach will not be efficient.

Floor tiles with different CFM rates are useful in establishing efficient airflow, ensuring sufficient cooling is presented to each cabinet.

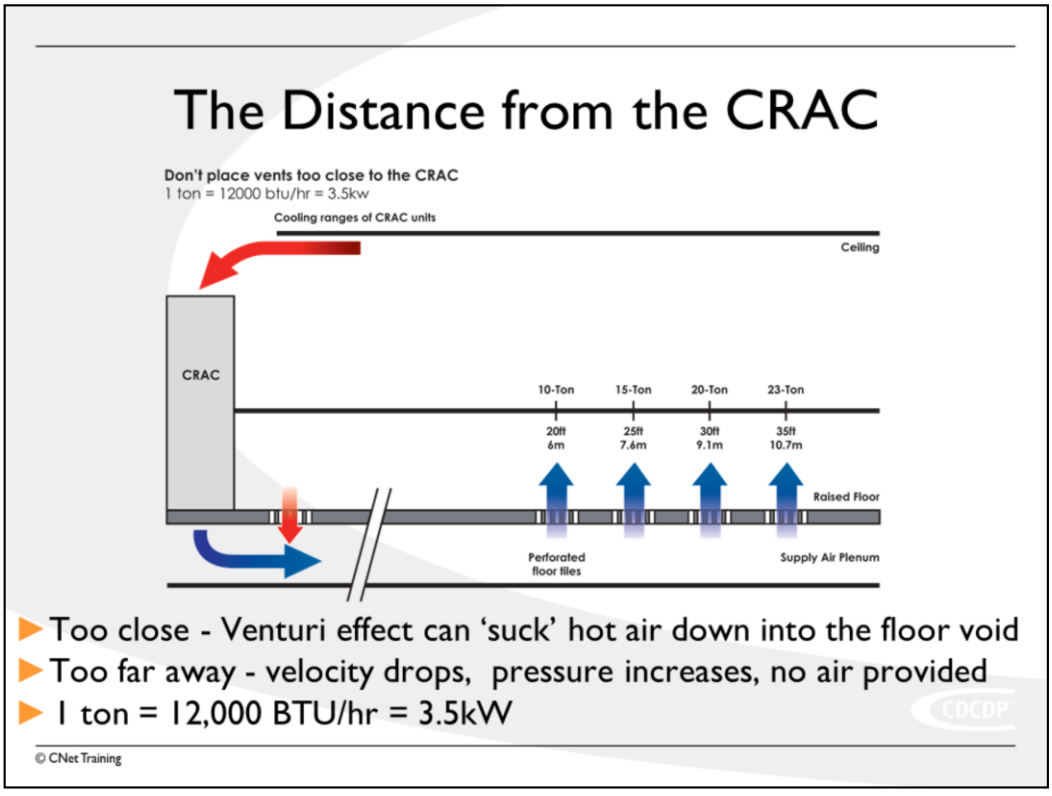
Assuming a static pressure of 25Pa, one highly ventilated floor tile will pass enough air to cool around 5kW.



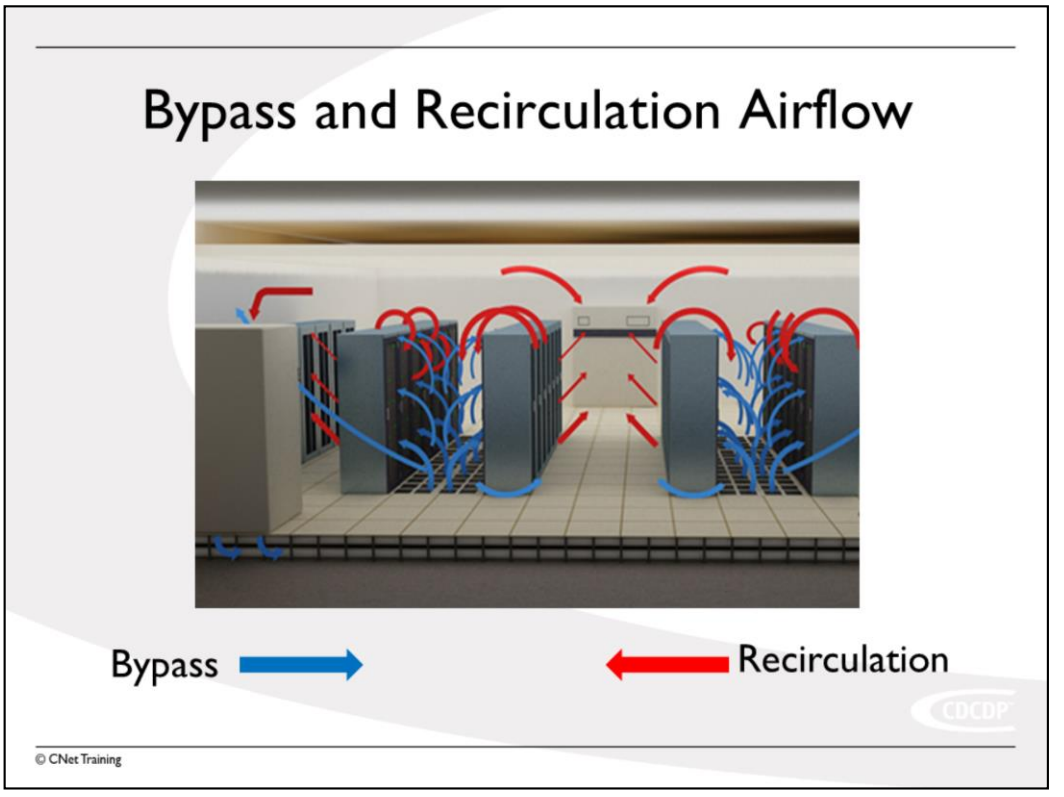
With directional airflow panels being incorporated into cold aisle containment or semi-contained aisles (aisle doors only), more precise cooling can be delivered to the air intake of the equipment. Advanced versions are aligned to cabinet sensors, allowing different directional deliveries in zones from the bottom to the top of a given cabinet (as illustrated above). This has significant benefits:

- When more air is captured at the cabinet, it can cool higher-density loads because more air is reaching the intended target.
- When air delivery from a tile becomes more precise, it no longer needs as much volume as historically required. Less air to move = Fewer cooling units or slower fan speeds
- When combined, these increase the delivery of precision cooling to cabinets greater than 10kW load density.

Source: http://tateairflow.com/airflow-panels



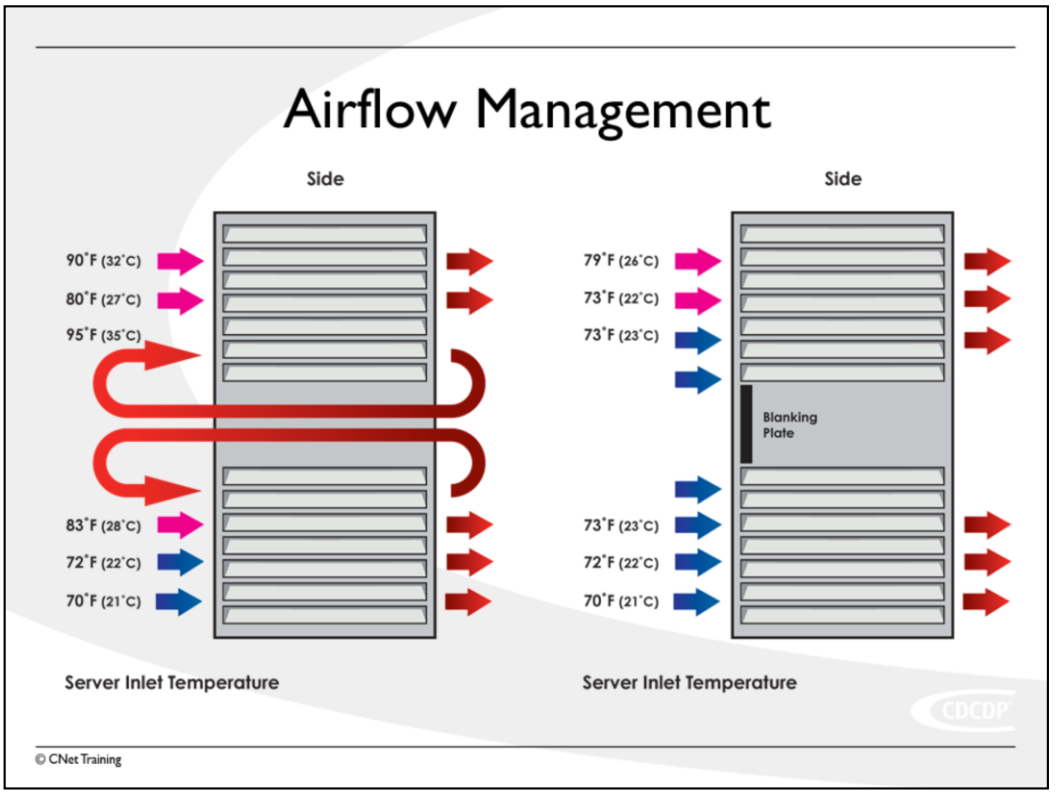
Guidelines exist showing the size CRAC required to cool over various distances. Typically, the most effective cooling begins about 8ft (2.4m) from the CRAC unit. Although units with capacities greater than 20 tons are available, the increased heat density of today's servers limits the cooling range to approximately 30ft or 9.1m.



Definitions:

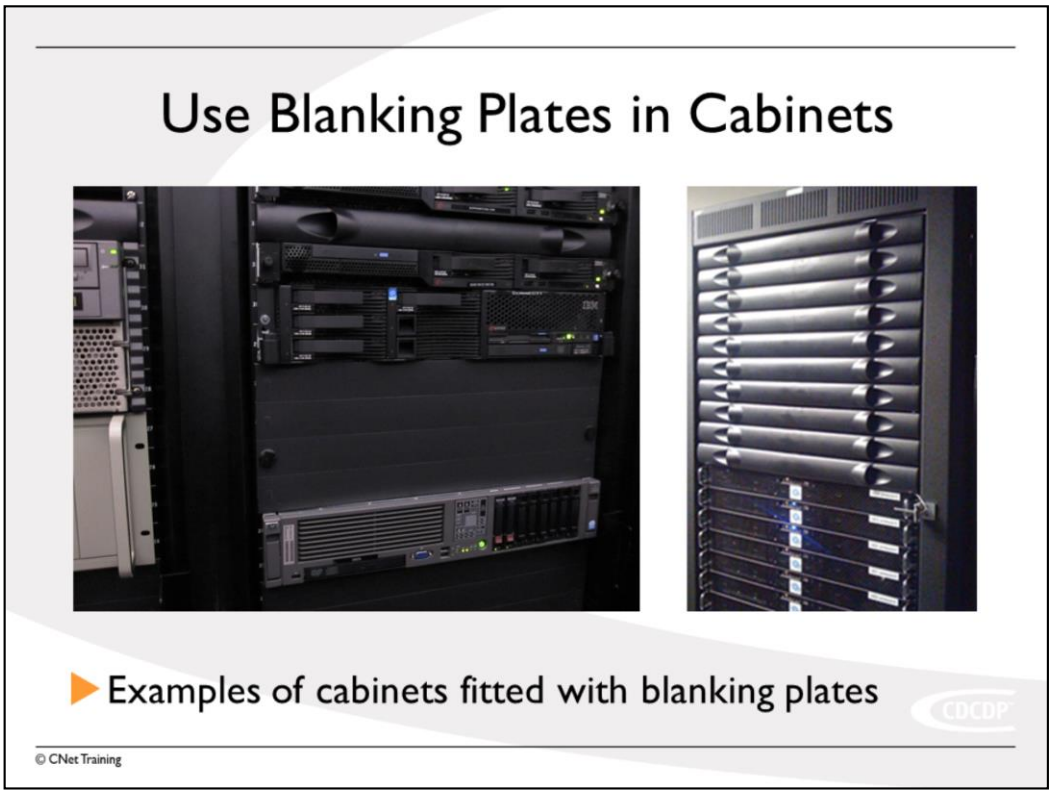
- **Bypass air** - Conditioned air that does not reach computer equipment, escaping through cable cut-outs, holes under cabinets, misplaced perforated tiles or holes in the computer room perimeter walls; limits the precise delivery of cold air at the server intake.
- **Hot air recirculation** - Where waste heat enters the cold aisle, requiring the cooling infrastructure to supply colder air at the equipment to offset this mixing.

These are key factors the CDCD must minimise during design considerations for the cooling system and airflow management cycle.



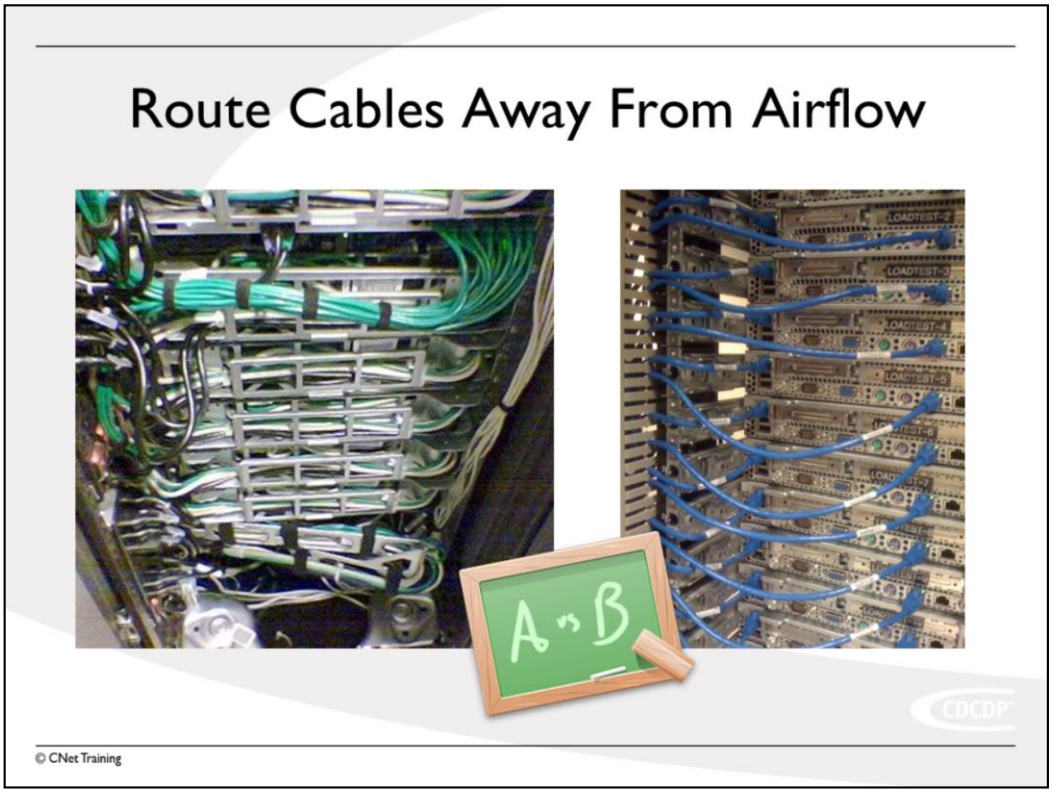
Open gaps and spaces are a major cause of poor airflow management. This should be prevented wherever possible by:

- Blanking plates in cabinets between equipment
- Using side air dams on wide cabinets
- Using brush grommets for cables
- Avoiding shelf-mounted equipment
- Having ventilated front and rear doors

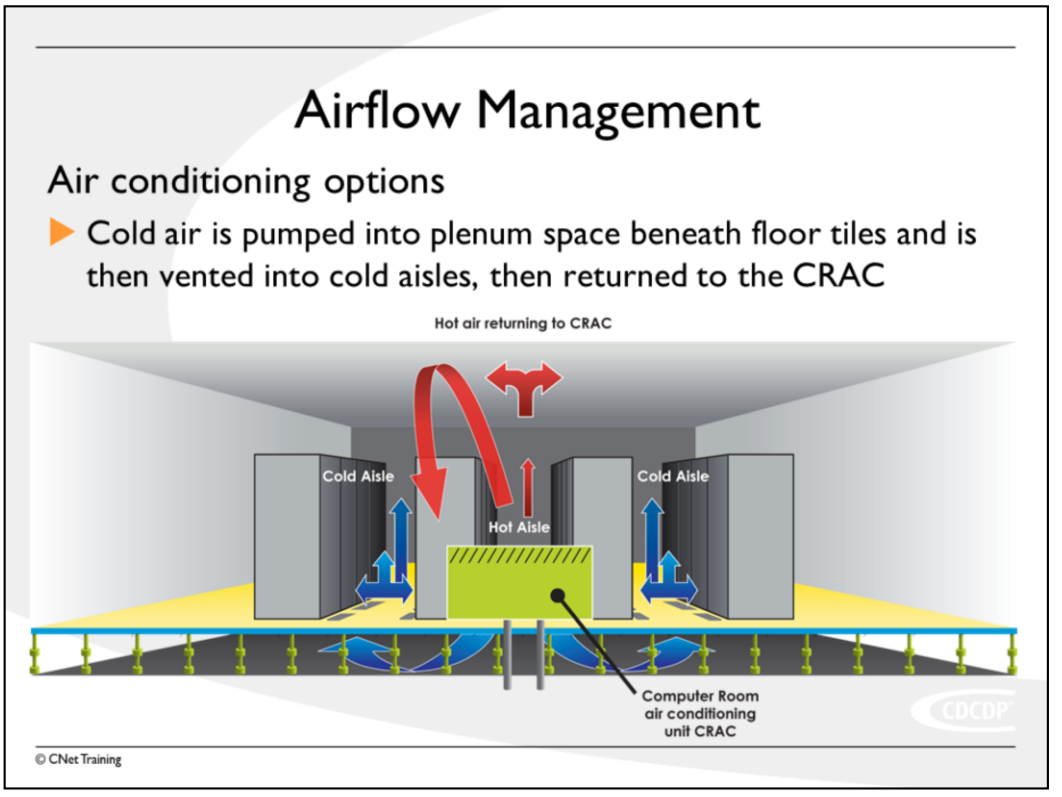


It is important to blank off any bypass routes the air could flow through, even in cabinets where there is little or no equipment. There are now many differing forms of blanking plates available from vendors with strip and fit plenaform, to plastic inserts, to steel blanking plates. Each has varying design qualities, which the CDCD should evaluate for the most practical design and cost-effective solution.

Air flowing through cable access holes into cabinets and through walls must be sealed correctly. The CDCD must assess the merits of each product to ensure they are appropriate for the designated installation task. It should be noted firestop seals will need to be evaluated against local fire regulation specifications.



Cables can and do impede airflow, so they must be routed correctly to minimise this effect.

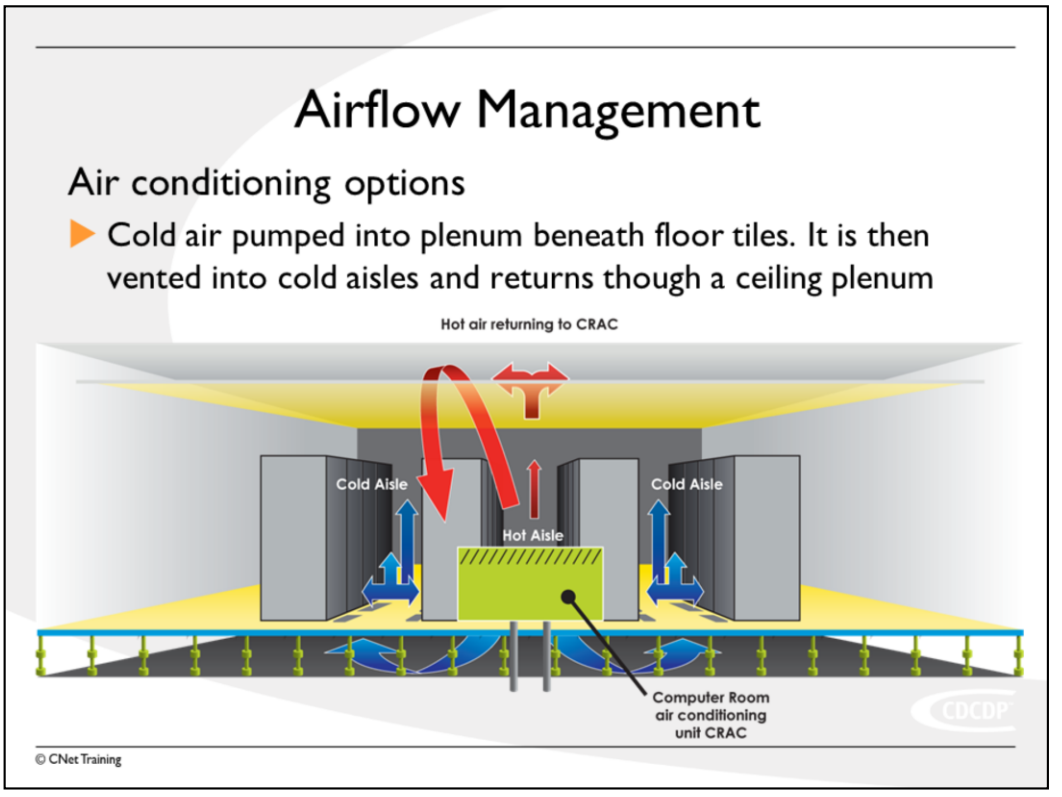


Standards traditionally recommend the hot aisle-cold aisle layout as shown.

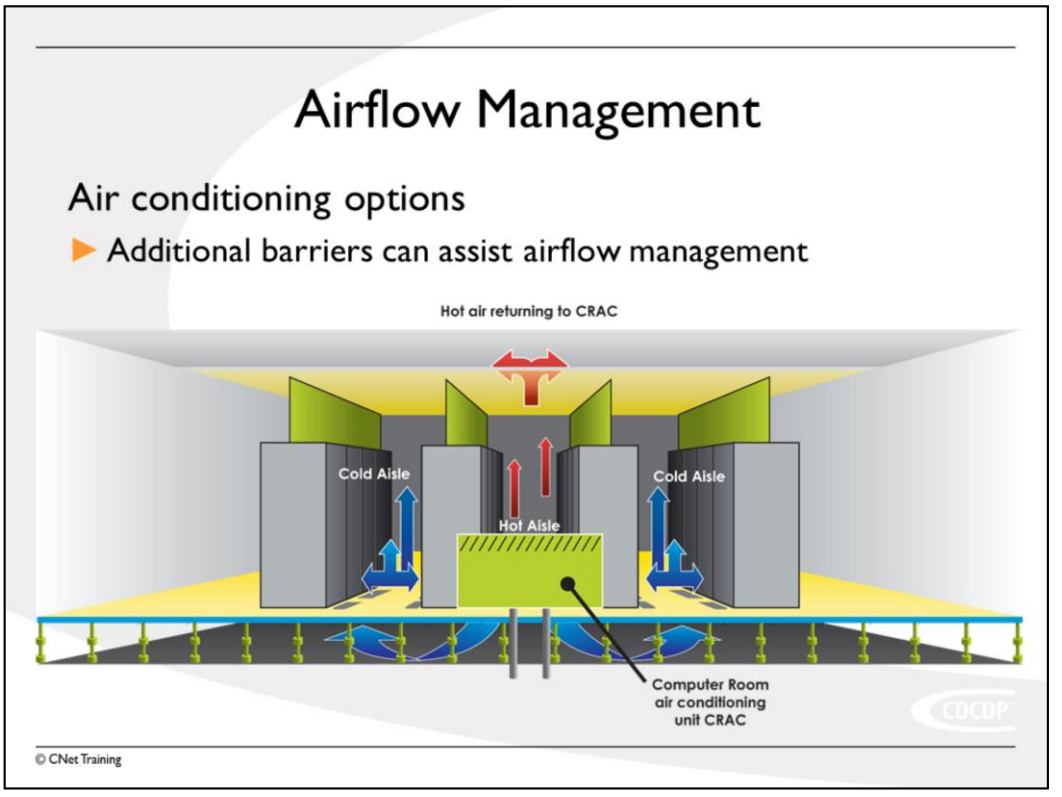
This simple layout relies on natural convection to return the hot air to the CRAC unit.

With a one-to-one relationship between cabinet fronts and ventilated tiles in the cold aisle, there can be a limitation to ~5kW per rack.

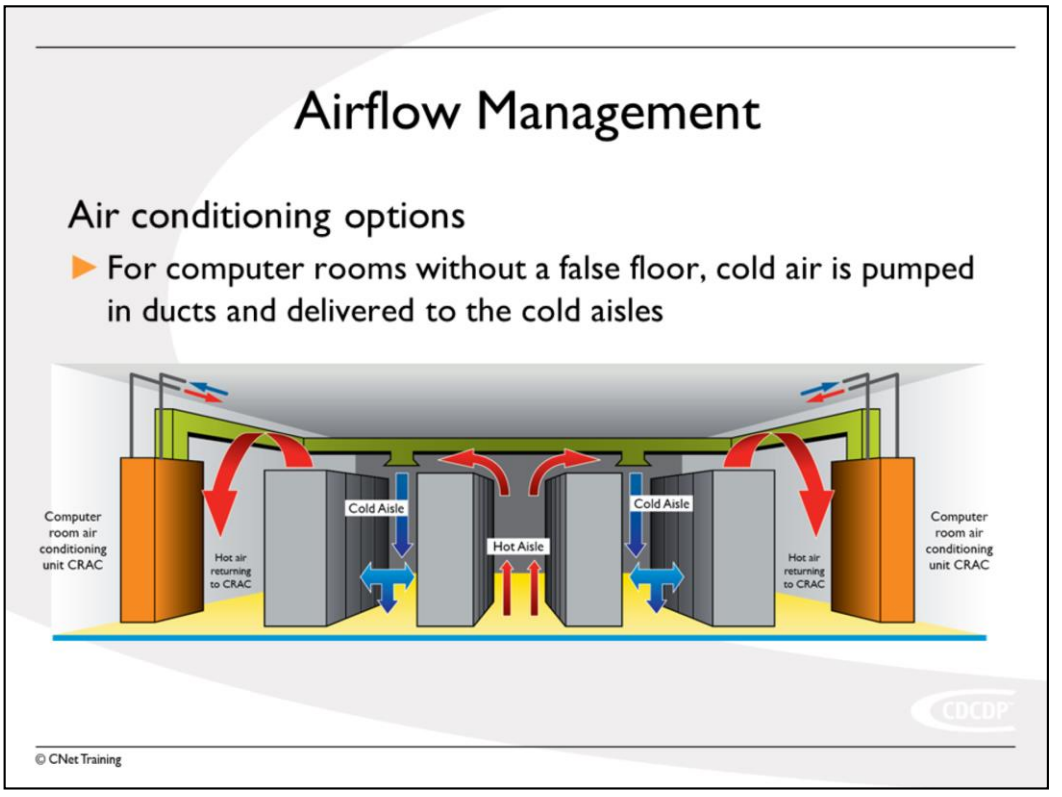
Managing the airflow from the hot aisle to the CRAC is left to natural convection in the room.



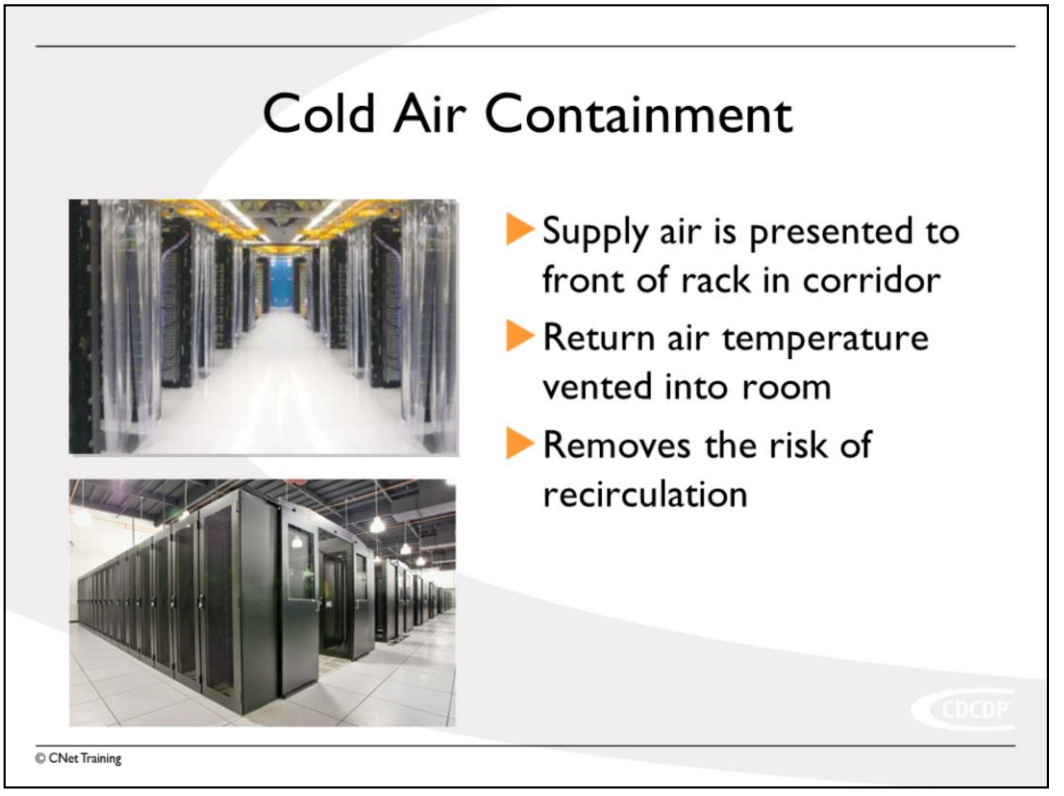
The performance of this simple layout can be enhanced by managing the return airflow to the CRAC. In this example, using a false ceiling with vents above the hot aisle acts as a return plenum.



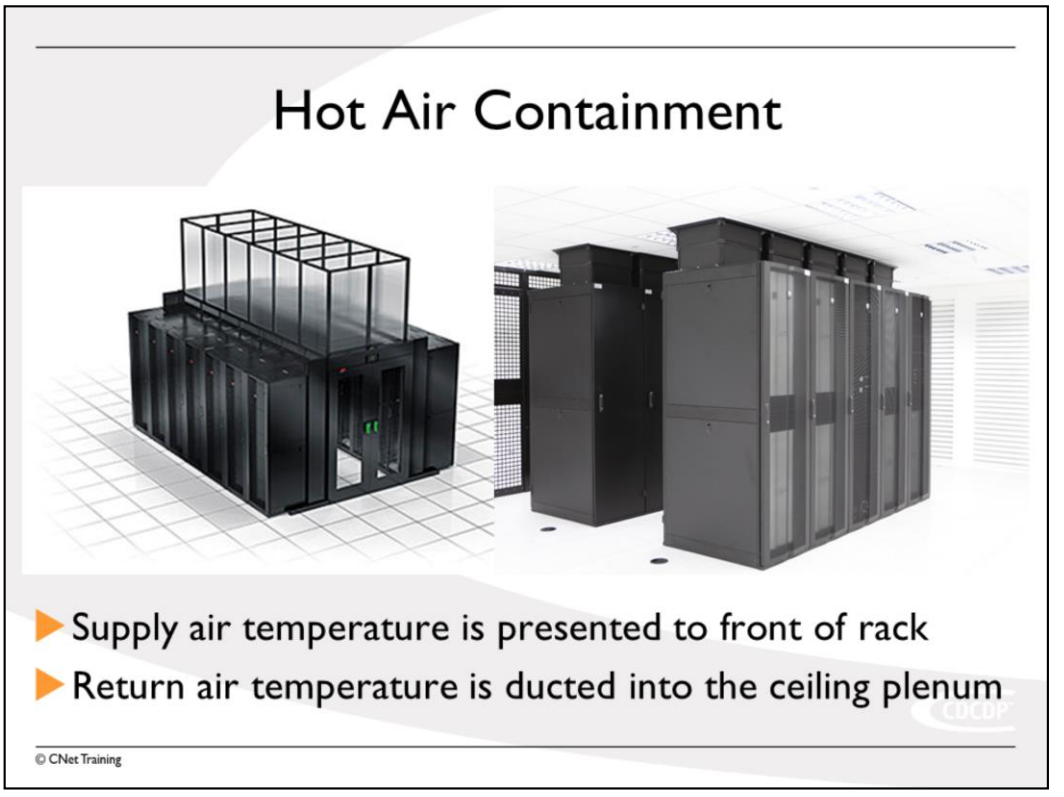
In this example, additional barriers make sure the hot air is directed into the ceiling plenum. The barriers must close the gap between the top of the racks and the ceiling.



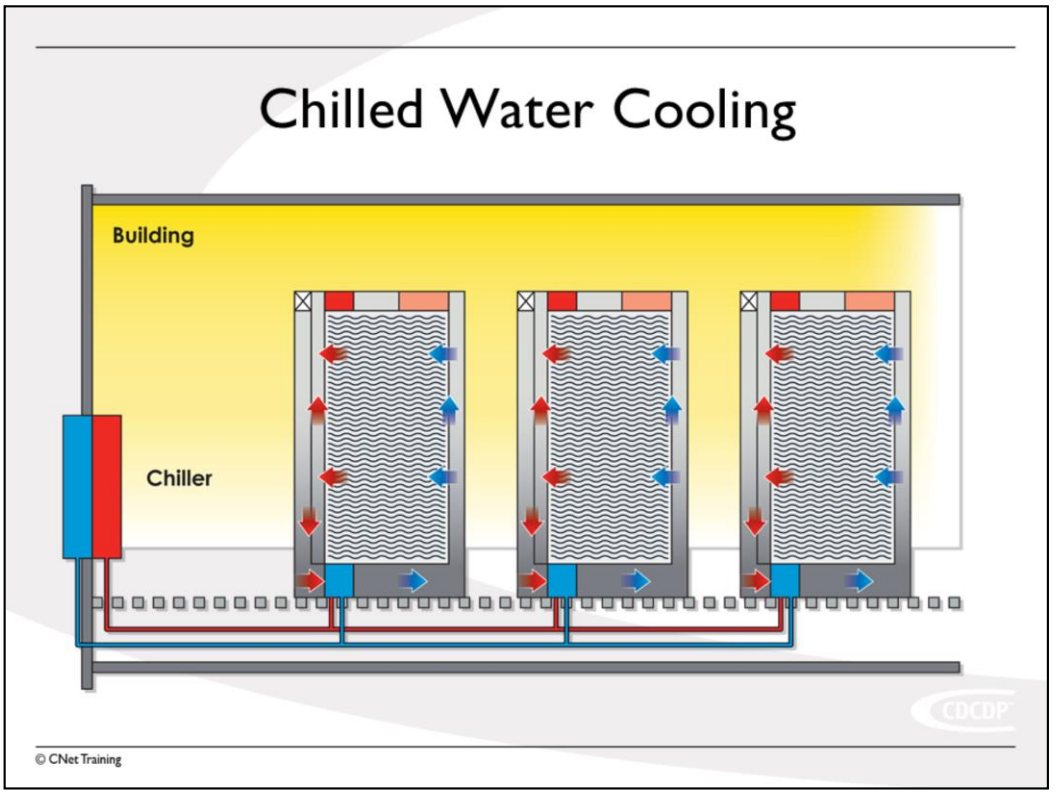
Note: Ductwork imposes friction, and may decrease efficiency unless sized correctly due to increased fan loads.



When a raised access floor is present, it is recommended cold aisle containment is introduced, to maximise the potential of the underfloor cooling system.



Hot aisle containment and cabinets with installed chimneys allow the return air temperature to be captured at source. It is then directly routed into the ceiling plenum.



Just as with an air system, the challenge is to remove heat from the computer room to somewhere else. This is achieved simply, as shown, by piping the warmed water through a chiller and returning it as chilled water.

These systems are either closed-loop, or they are open at the cold aisle side. They can be used in a mixed environment in a hot aisle-cold aisle room.

Another advantage of water is that 'it's just plumbing'. Accordingly, the skillset to work on these systems is widely available and repairs are relatively easy.

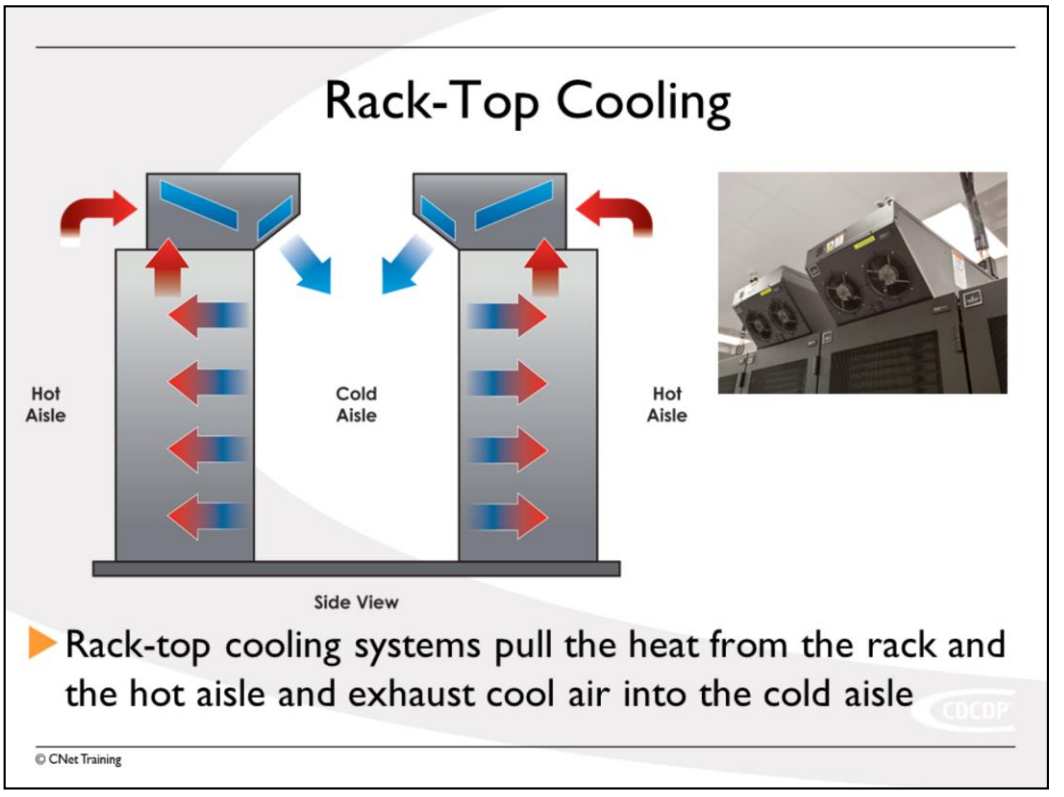
One problem with water cooling: It is not easy to size correctly for variable power loads. The system has a fixed capacity, so it is difficult to scale; hence, it is often oversized and has a price premium.

Cabinet Mounted Cooler

- Rear-mounted
  - Compatible with all cabinets
  - Does not include cabinet
  - Fitted to cabinet rear door
    - 50% free area
  - High capacity cooling
  - 600mm wide x 42U = 20kW
  - 800mm wide x 47U = 30kW
  - Target 40kW+

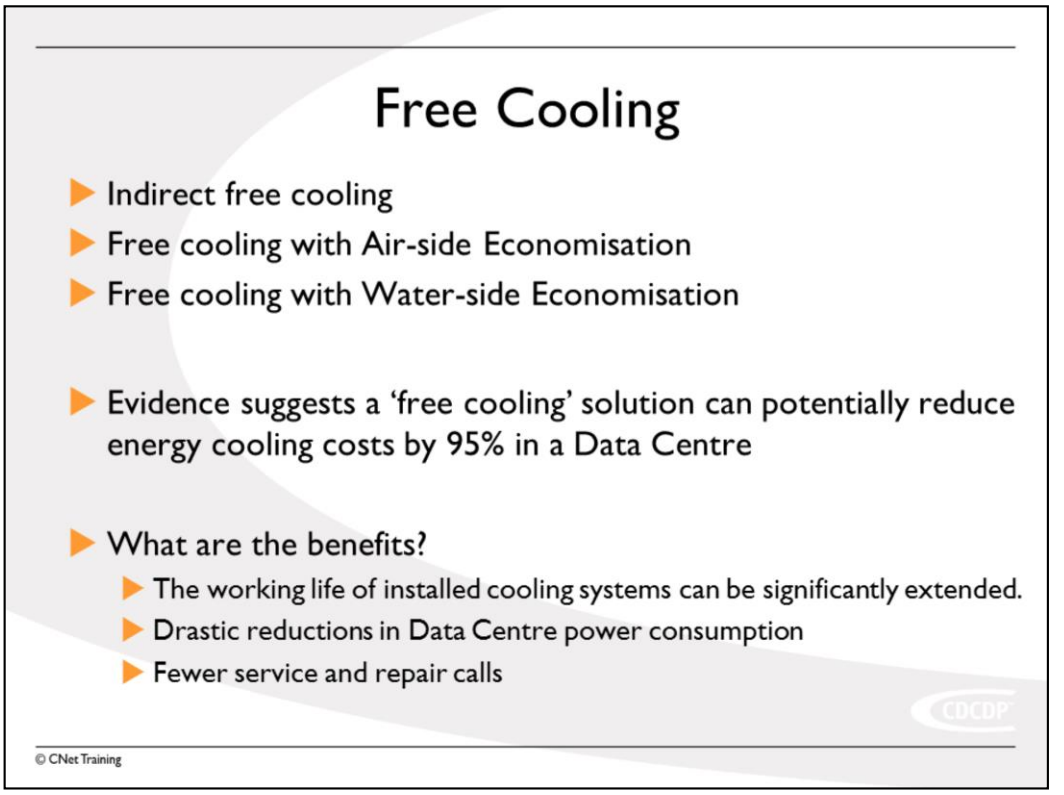
© CNet Training

Rack cooling can be used where needed but as the air exhausted at the rear of the cabinet is cooled, it can not be integrated in a standard hot aisle-cold aisle scenario. Introducing more fans into the facility could falsely increase the measured IT load, depending on meter points.



Rack-top units can be used to cool down hot air and recycle it into the cold aisle. These require some means of transferring the heat from the rack-top unit to the outside of the Data Centre, which could be CO_2, water, etc.

These exhaust into the cold aisle, so they can be used to augment a hot aisle-cold aisle room. They will also introduce more fans into the facility.



Put in simple terms, free cooling harnesses external environmental conditions (e.g., air and water) to cool a Data Centre. More often than not, especially in the UK, the prevailing air temperature will be considerably cooler than the air warmed by Data Centre equipment (The Green Grid and ASHRAE provide global weather patterns to highlight the air-side and water-side economisation potential).

By filtering, humidifying and introducing this air directly into the Data Centre, it is possible to reduce or eliminate the use of industrial-grade CRAC systems. Cooling systems that use this approach are sometimes called air-side economisers.

Alternatively, a source of cold water from local rivers, lakes or underground sources can be circulated (once cleansed) into a Data Centre and used instead of undergoing the traditional method of refrigerating a closed water loop with a chiller. Systems using this approach are often called water-side economisers and are typically used to cool either room air, or funnelled directly to cool cabinets and other systems. (Source: 2bm)

Note: Economisation and free cooling will be addressed in further detail during the Professional cooling modules

Free Cooling Savings Profile

Total energy consumption of environmental control system	W
Total number of hours per year	8,760
Number of hours of matching conditions during year	H
Energy consumption fraction of environmental cooling system made inactive during periods of matching conditions	F
% of potential free cooling per year	P
Savings	R
% of potential free cooling	P=(H/8,760)
Savings on cooling	R=PxWxF

- The potential of utilising free cooling is now a major design consideration that should be fully assessed

Source: ETSI

© CNet Training

Free cooling is now a significant design consideration linked to the total reduction of energy usage and the external climatic environment. The reduction is directly proportional to the total period during which the external environmental conditions match the ideal combination of the Data Centre's operating parameters.

It should be noted free air cooling is supplementary to the fixed cooling infrastructure. 100% matching climatic conditions does not correspond to 100% reduction of energy consumption; the remainder of the cooling infrastructure (such as CRACs, CRAHs, chillers, fans and pumps) still consumes a level of energy (albeit a very low one) whilst free cooling opportunities are available.

Design Considerations

- Fully understand the range of equipment operating parameters
- Correctly address high-density environments, especially if they are only a low percentage
- Capability and flexibility to match technology advances
- Opportunity to utilise free cooling
- Utilisation of hot and cold aisle containment
- Understand how maintenance requirements will be supported
- Potential benefits of modular design
- Installation of high-efficiency components

CDCDP

© CNet Training

Review

- Can you?
  - Understand the applicable Standards
  - Understand the primary purpose of cooling
  - Identify the key cooling components
  - Discuss cooling options

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 5

© CNet Training

Certified Data Centre Design (CDCD®) Core Unit

Earthing and Bonding

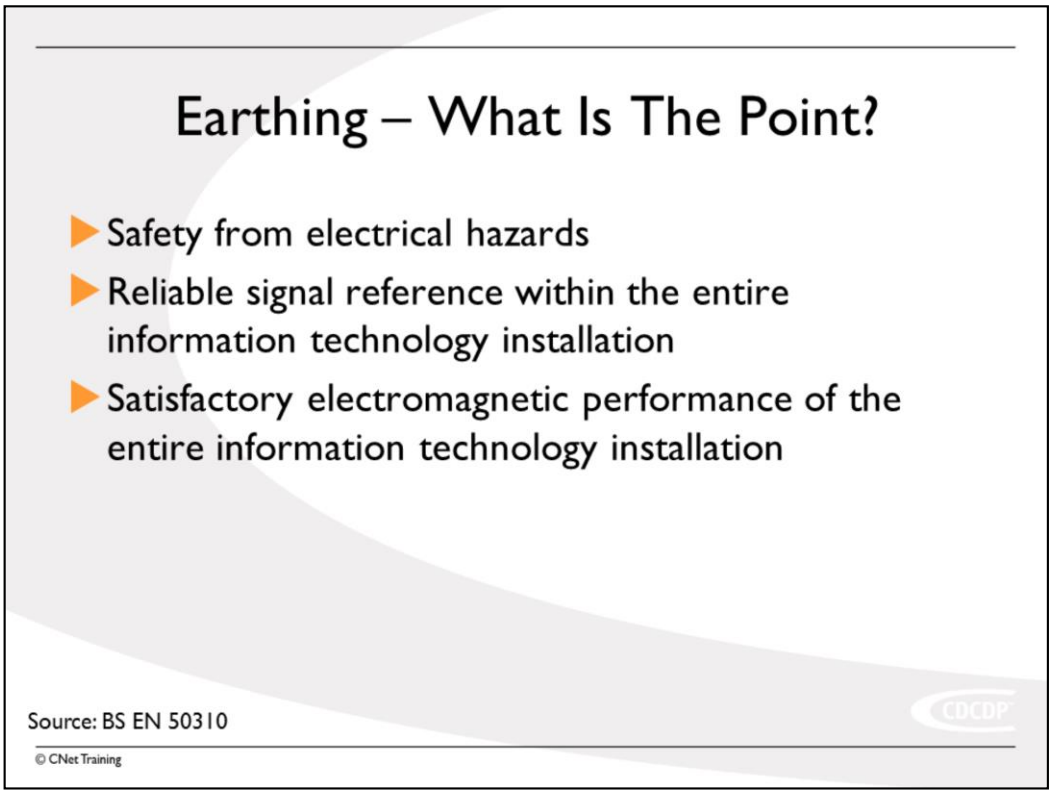
Version 1509

CDCDP

Objectives

- At the end of this module you will be able to:
  - Understand the need for earthing and bonding
  - Identify the applicable Standards
  - Describe the purpose of the signal reference grid (SRG)

© CNet Training



Earthing has a number of objectives. The primary requirement is to ensure safety from electrical hazards, something that is established in law.

UK

- SI 1989 No. 635: The Electricity at Work Regulations is statutory law in the UK. Any person or organisation found guilty of a breach could face prison.
- The Electricity at Work Regulations state in **Regulation 8 - Earthing or other suitable precautions,** that:
  - *"Precautions shall be taken, either by earthing or by other suitable means, to prevent danger arising when any conductor (other than a circuit conductor) which may reasonably foreseeably become charged as a result of either the use of a system, or a fault in a system, becomes so charged; and, for the purposes of ensuring compliance with this regulation, a conductor shall be regarded as earthed when it is connected to the general mass of earth by conductors of sufficient strength and current-carrying capability to discharge electrical energy to earth."*

USA

- The NEC Article 250 contains comprehensive details of grounding requirements in a wide range of circumstances.

Applicable Standards

- **IEC and ISO**
  - **IEC 60364-1** Electrical installations of buildings, various sections including Part 5-548: Earthing arrangements and equipotential bonding for information technology equipment
  - **ISO 11801:2002** Information technology – Generic cabling for customer premises
- **ETSI and ITU**
  - **ETS 300 253** Equipment Engineering – Earthing and bonding of telecommunications equipment in telecommunication centres
  - **ITU-T K.27** Bonding configurations and earthing inside a telecommunications building
  - **ITU-T K.31** Bonding configurations and earthing of telecommunications installations inside a subscriber's building

© CNet Training

There are IEC and ISO Standards. There are also many recommendations from bodies including ETSI and ITU.

Applicable Standards

Europe

- **EN 50310:** Application of equipotential bonding and earthing in buildings with information technology equipment
- **EN 50174-2:** Information technology – Cabling installation Part 2: Installation and planning practices inside buildings

UK

- **BS 7671:** Requirements for Electrical Installations: IET Wiring Regulations 17th Edition (BS 7671:2008+A3:2015)
- **BS 6701:** Telecommunications equipment and telecommunications cabling. Specification for installation, operation and maintenance

© CNet Training

- Europe has EN Standards.
- The UK has BS Standards.

Applicable Standards

USA

- **NEC Article 250**
- **TIA-607-B:** Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises
- **IEEE STD 1100-2005:** Recommended Practice for Powering and Grounding Electronic Equipment

© CNet Training

The USA has its own Standards.

Terminology

- **Earthing:** The connection of the exposed conductive parts of an installation to the main earthing terminal of that installation (BS 7671)
- **Equipotential bonding:** The electrical connection putting various exposed conductive parts and extraneous conductive parts at a substantially equal potential (EN 50174-2)
- **Grounding (USA):** A conducting connection, whether intentional or accidental, between an electrical circuit and the earth (TIA 607-B)

© CNet Training

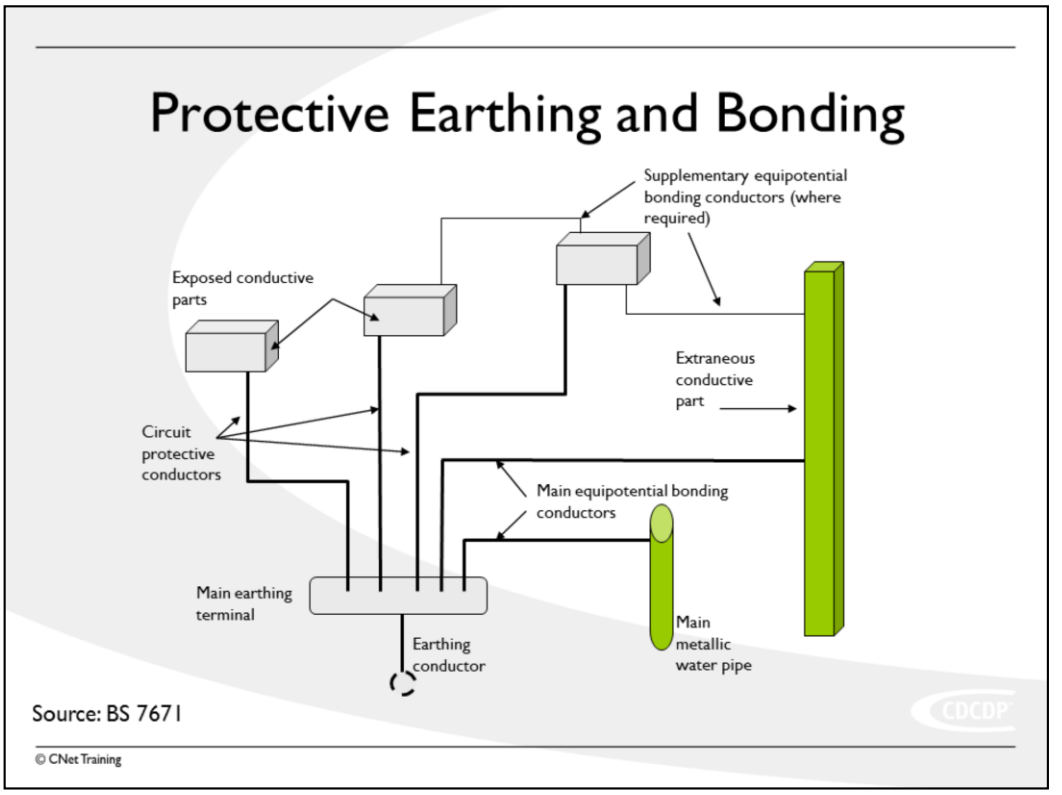
- Terminology varies between the different Standards.
- Earthing and grounding are used interchangeably.

Bolting it all Together: The Equipotential Bonding System

- In an installation, main equipotential bonding conductors shall connect extraneous conductive parts of that installation to the main earthing terminal, including the following:
  - Water service pipes
  - Gas service pipes
  - Other service pipes and ducting
  - Central heating and air conditioning systems
  - Exposed metallic structural parts of the building
  - The lightning protection system
  - The metallic sheath of any telecommunications cable

© CNet Training

In any electrical system in a building, it is necessary to create a Faraday Cage where all exposed metalwork is bonded together.



- BS 7671 defines the terms used in the UK and Europe
- EN 50310 2010 defines terms used in Europe

Definitions:

- **Equipotential bonding:** Electrical connection maintaining various exposed conductive parts and extraneous conductive parts at substantially the same potential
- **Exposed conductive part:** Conductive part of equipment which can be touched, and which is not normally live, but can become live when basic insulation fails
- **Extraneous conductive part:** A conductive part not forming part of the electrical installation, and liable to introduce an electrical potential, generally the electric potential of the local earth.

Main Equipotential Bonding Conductor

- **BS 7671**
  - The main equipotential bonding conductor shall have a cross sectional area not less than half the CSA of the earthing conductor. It shall not be less than $6mm^2$ and need not be more than $25mm^2$ if made of copper.
  - The supplementary equipotential bonding conductor shall not be less than $4mm^2$ where no mechanical protection is provided, or $2.5mm^2$ where protection is provided.
- **TIA 607**
  - Calls for a minimum 6 American Wire Gauge (AWG) grounding conductor
    - 4.1mm in diameter, $13.2mm^2$

© CNet Training

The earthing conductors need to have a low electrical resistance, so minimum sizes are specified.

Protective Conductor Identification

Europe

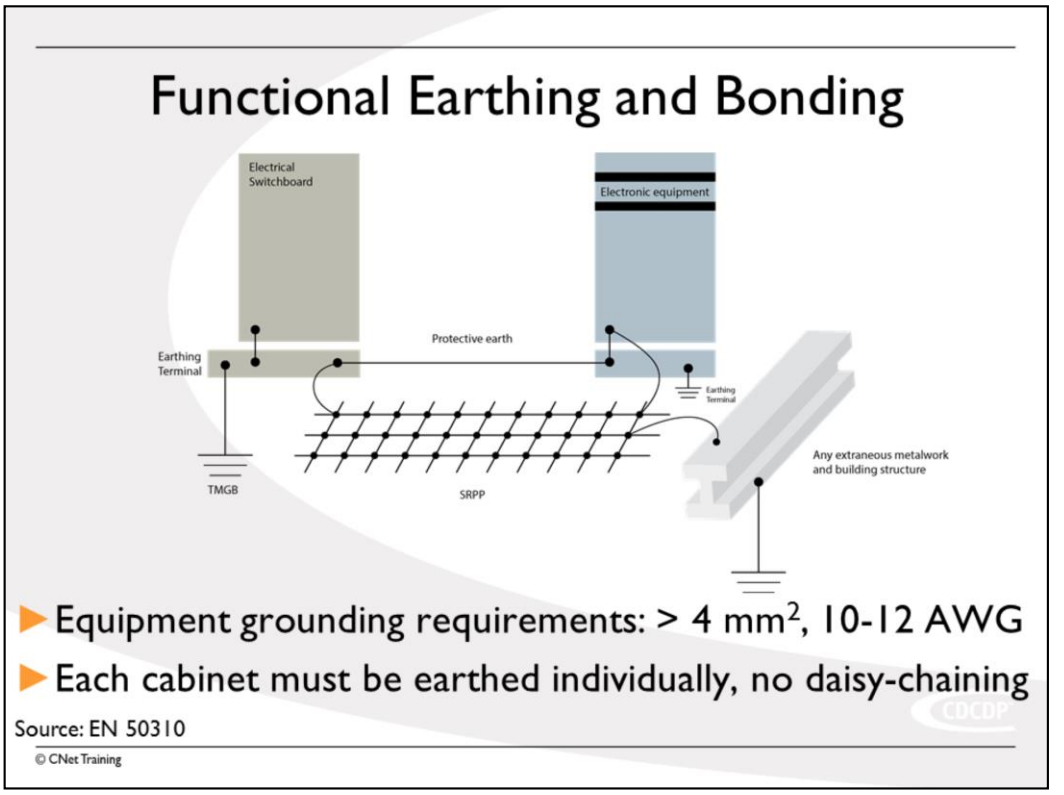
- The colour of all protective conductors shall be green and yellow
  - IEC, BS 7671

USA

- For conductors 6 AWG and smaller, the equipment grounding wire is identified by green outer finish or green with yellow stripe(s)
  - NEC Article 250

© CNet Training

Earthing conductors shall be positively identified.



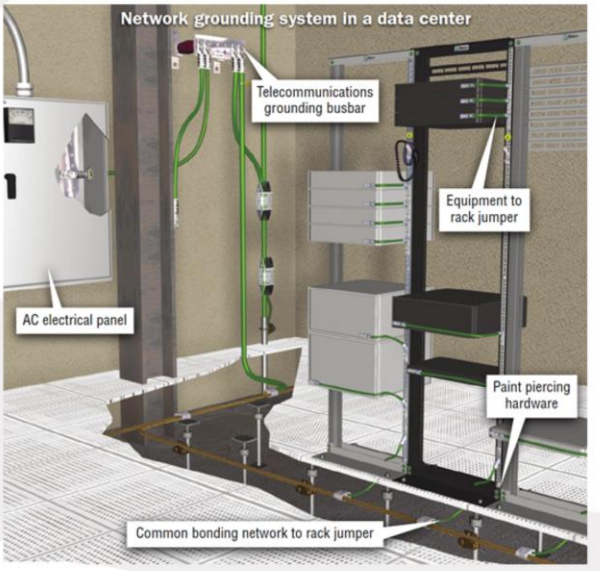
Integrity of referenced conductors

If a circuit conductor is connected to earth, or to any other reference point, nothing which might reasonably be expected to give rise to danger by breaking the electrical continuity (or introducing high impedance) shall be placed in that conductor, unless suitable precautions are taken to prevent that danger.

What this means in practice in the Data Centre is <u>each</u> cabinet must have a dedicated connection back to a main earthing terminal, or to a suitable system reference potential plane (SRPP); daisy-chaining is not allowed. It also means doors and side panels must all be electrically connected.

As a point of note, the CDCD must be aware of different terminologies between Standards and regulatory-based documents, especially in regard to protective and functional earthing. This is a prime example of why an electrical engineer should be on the design team.

Network Grounding System



PANDUIT™

CDCDP

© CNet Training

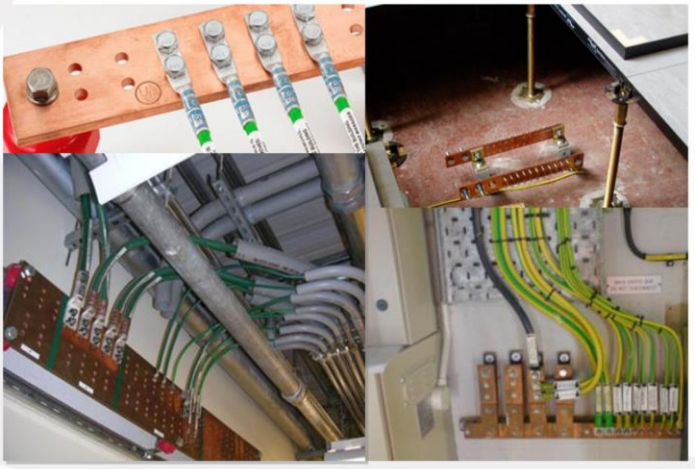
Potential Difference to Earth

- ISO 11801 requirements
  - Earthing and bonding shall be in accordance with applicable electrical codes or IEC 60364-1
  - The building earthing system should not exceed the earth potential difference limits of 1 volt rms

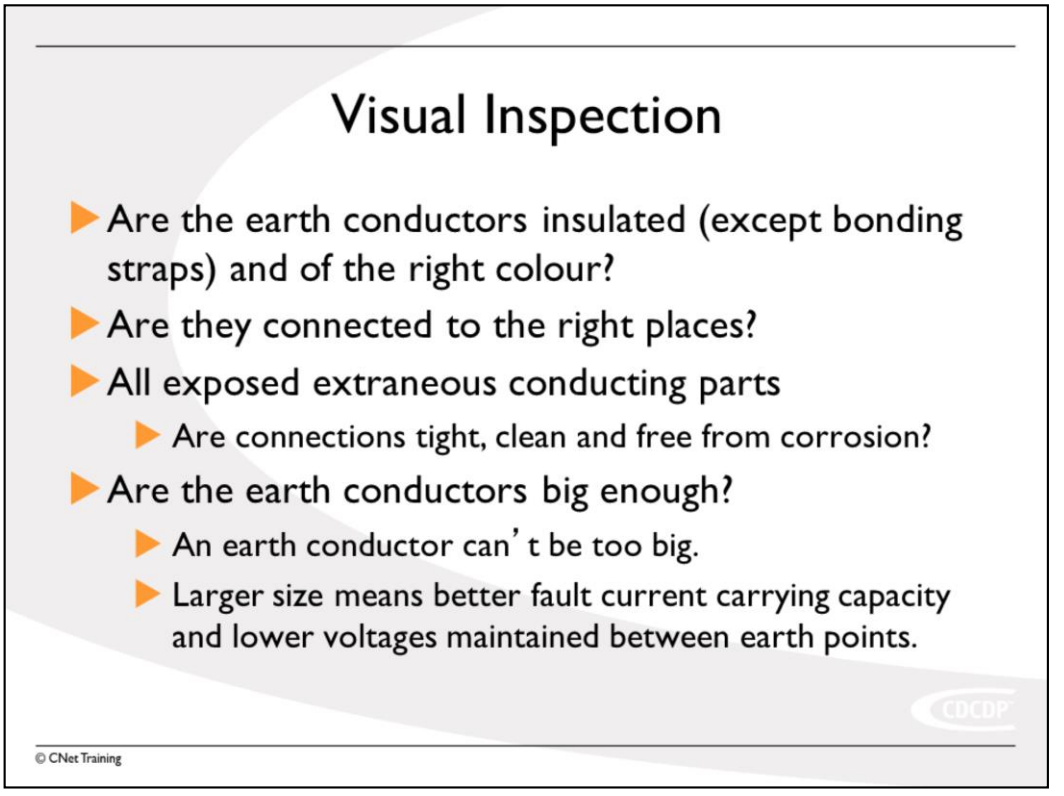
© CNet Training

The communications Standards set limits on the voltage rise of the system with respect to earth.

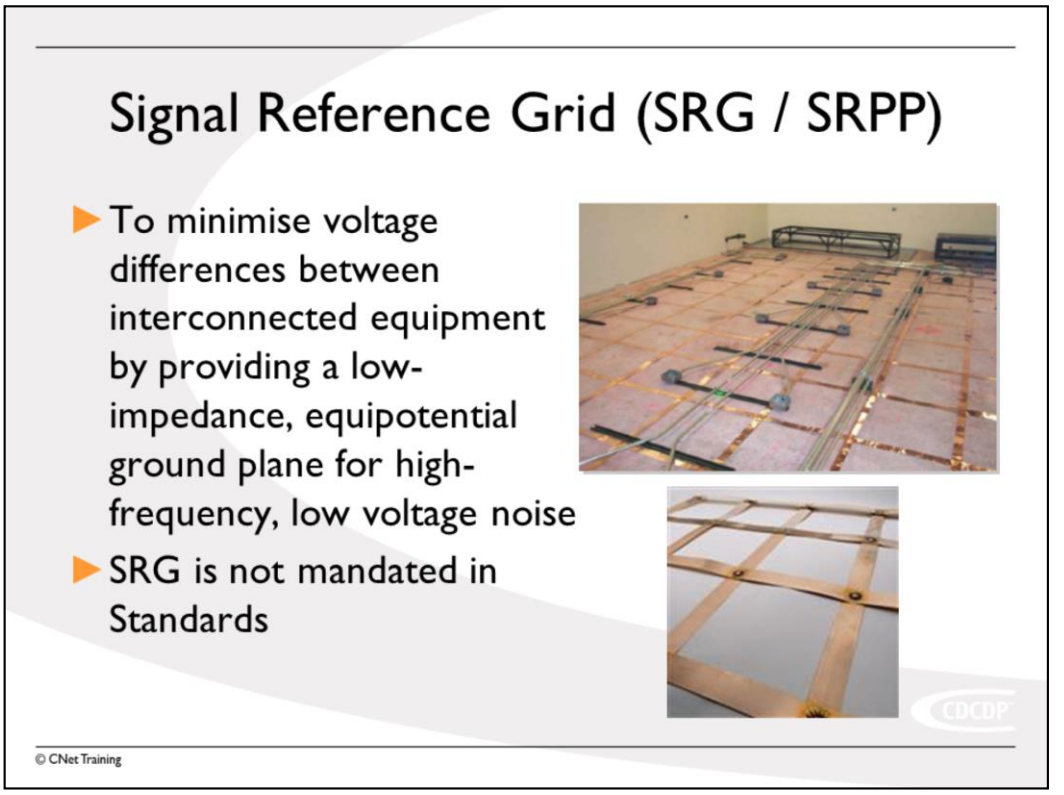
Examples of Earth Bar Connectivity



© CNet Training



It is important that earthing systems are inspected. A visual inspection can tell a lot.



In a Data Centre, it is necessary to minimise electrical interference. The purpose of the earthing conductors discussed so far has been electrical safety and conducting potentially large fault currents to earth. In a Data Centre, there is an additional requirement.

A Data Centre contains many (tens or hundreds) power supplies, in items such as servers and switches, each of which generates high frequency current, which is dumped to earth so it doesn't reach the DC side. A conductor which presents a very low impedance (e.g., 1 Ohm) to mains frequencies (50 or 60Hz) may look like a relatively high impedance (200-300 Ohm) to high frequency noise currents.

In order to satisfactorily conduct these noise currents to earth, a larger cross-sectional area conductor is required. An SRG made from copper tape is one means of achieving this, by providing many parallel paths for noise currents.

SRG is often referred to as a system reference potential plane (SRPP) in Europe.

There are no current Standards which mandate the use of a SRG, though EN 50310 suggests it is good practice: *"[SRPP…] as an ideal goal in potential equalising, is approached in practice by horizontal or vertical meshes."*

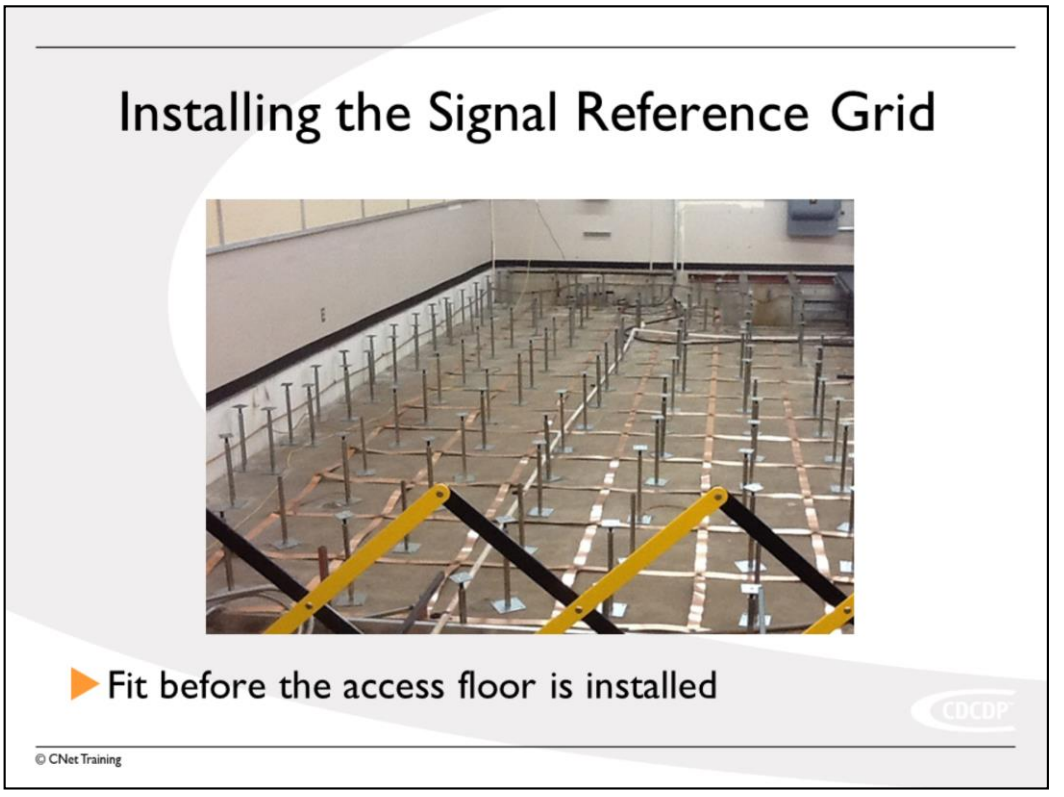
SRG (SRPP) – An Ideal Goal?

BS EN 50310

- SRPP conductive solid plane, as an ideal goal in potential equalising, is approached in practice by horizontal or vertical meshes. The mesh width thereof is adapted to the frequency range to be considered. Horizontal and vertical meshes may be interconnected to form a grid structure approximating a Faraday Cage.

© CNet Training

As the data rate increases, the size of the SRG mesh should decrease. At 10 Gigabit Ethernet, some recommendations state a 10cm (4in) mesh, which is extremely difficult to achieve.



There are many different opinions on the efficiency of the SRG and the size of its 'cells', but one thing is certain – it is easier to install before tiles are fitted.

The Manufacturer Views

- The high operating frequencies of modern computer equipment require computer room products be supported both by a good equipment grounding system and an effective SRG.
  Source: HP
- A signal reference grid should be designed for the computer room. This provides an equal potential plane of reference over a broad band of frequencies, through the use of a network of low-impedance conductors installed throughout the facility.
  Source: Oracle
- Access (raised) flooring systems that utilise bolted stringer construction can be used to provide a simple SRG. Floor systems that have either no stringer or snap-in stringers do not provide for an effective SRG, and other methods for installing an SRG should be used.
  Source: IBM

© CNet Training

Manufacturers have their own views.

SRG Considerations

- Choose conductor type as appropriate
- Higher data speeds can require a tighter SRG
- Bond the SRG to each piece of electronic equipment, and to any other electrical or mechanical equipment located on the SRG
- Bonding connections to the SRG should be as short as practical, with no sharp folds or bends
- Flexible straps (also referred to as flat straps) are preferred to the use of round conductors

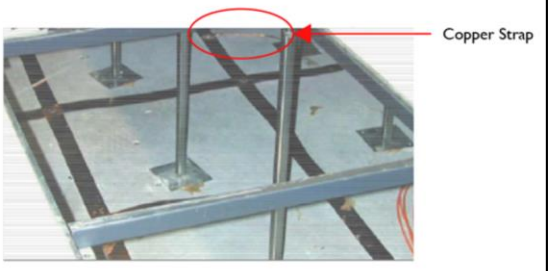
© CNet Training

Achieving an effective SRG is a complex matter. In addition to noise from power supplies, there are copper data cables transmitting high-speed data, which radiate high frequencies in the radio spectrum.

- The 600mm x 600mm (24in x 24in) SRG can cope with frequencies into the megahertz (MHz) range, but starts to struggle in the gigahertz (GHz) range.
- Higher data rates may require a tighter grid, and some recommendations claim a 100mm x 100mm (4in x 4in) SRG is required.
- EN 50310 says *"The mesh width [of SRPP], thereof, is adapted to the frequency range to be considered."*

Floor Pedestals

- Every sixth metallic raised floor pedestal needs to be bonded to the SRG. This helps bleed off static charges built up from the raised floor system. (BICSI 002)



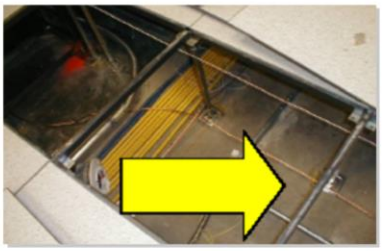
- EN 50174-2 suggests every two or three pedestals are earthed with a 10mm^2 wire

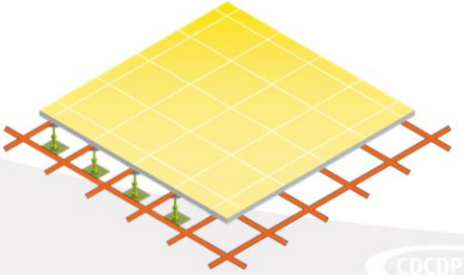
© CNet Training

This becomes more critical with higher speed data systems.

Conductor Types

- Round conductor
  - Easier to install when retrofitting an existing raised floor system
- Flat strip
  - Superior system
  - Less impedance than round conductors
  - Better performance at high frequencies
  - Less labour-intensive to install

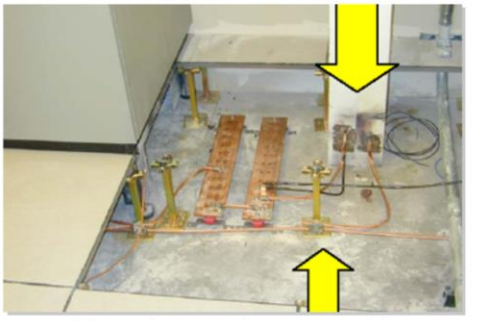




© CNet Training

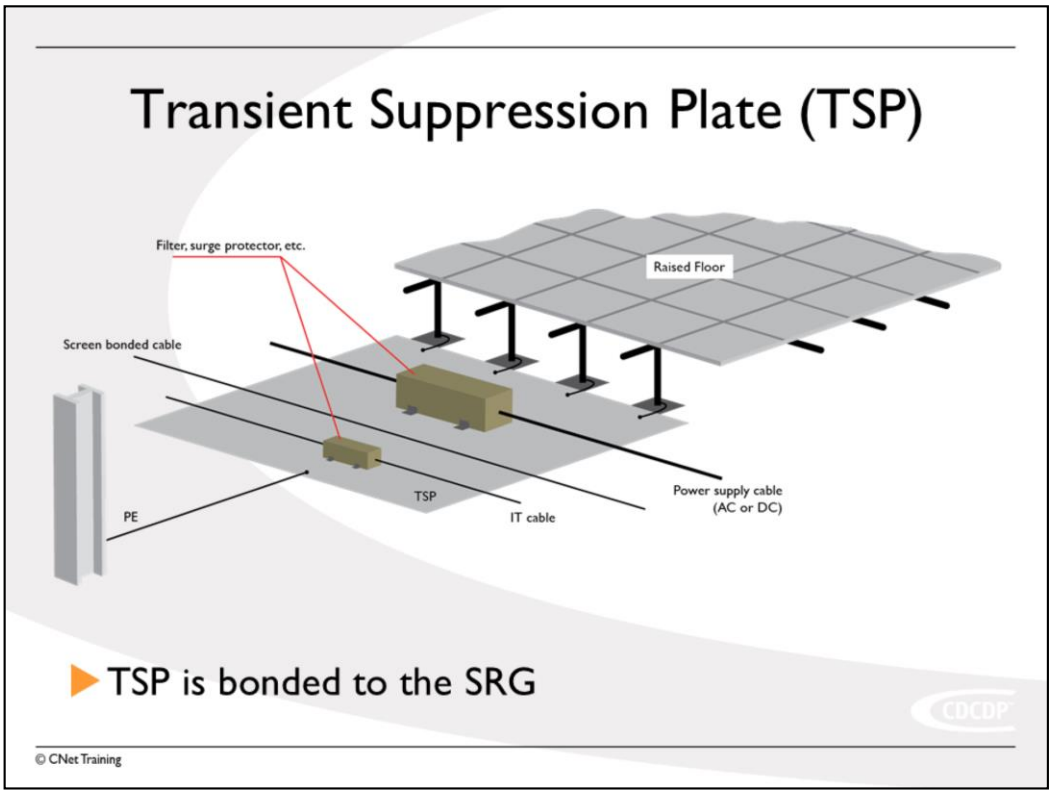
Bonding Connections

- Permanently and effectively bond the SRG to all accessible building steel, and to each metallic path (for example - conduits, raceways, cable trays, pipes and ducts) that crosses the SRG in any plane, or within 6ft (2m) of the SRG



Note the exothermic weld

© CNet Training



TSPs are sometimes fitted near equipment where electrical interference is likely, such as underneath PDUs.

The TSP is used as a potential reference, on which all electromagnetic interference (EMI) suppression components are bonded. These include filters, voltage suppressors and screened cables. A metal plate of 1m x 1m (minimum) is intended to divert noise current to reinforcing steel in the concrete under the raised floor.

Review

- Can you?
  - Understand the need for earthing and bonding
  - Identify the applicable Standards
  - Describe the purpose of the signal reference grid (SRG)

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 6

© CNet Training

Certified Data Centre Design (CDCD®) – Core Unit

Cable Containment, Management and Protection

Version 1509

CDCDP

Objectives

- At the end of this module you will be able to:
  - Understand the use of containment for good cable management, administration, protection and safety
  - Describe the different containment systems in use
  - State the separation distances between different services

© CNet Training

Cable Infrastructure Administration

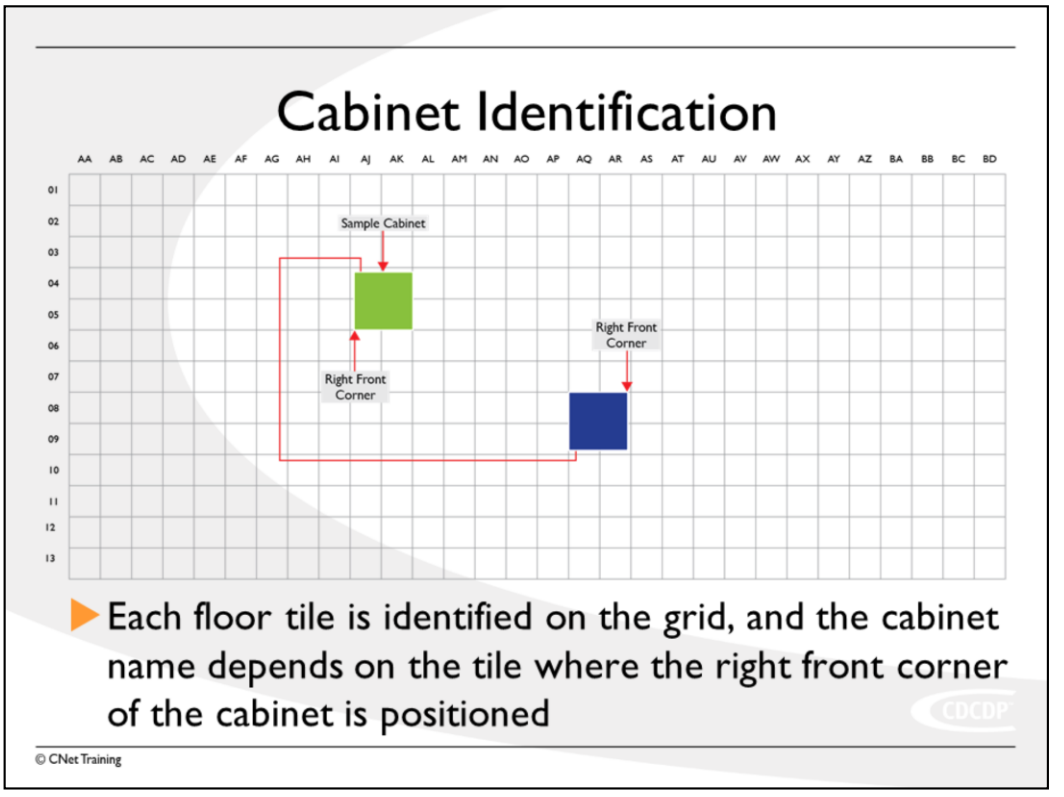
- All cables and components should be suitably marked to uniquely identify them
- The durability of all labelling must also be suitable for the rigours of the environment in which they are placed, and the expected timescale of the installation - usually in excess of 10 years
- Containment is a key contributor to good cable administration

© CNet Training

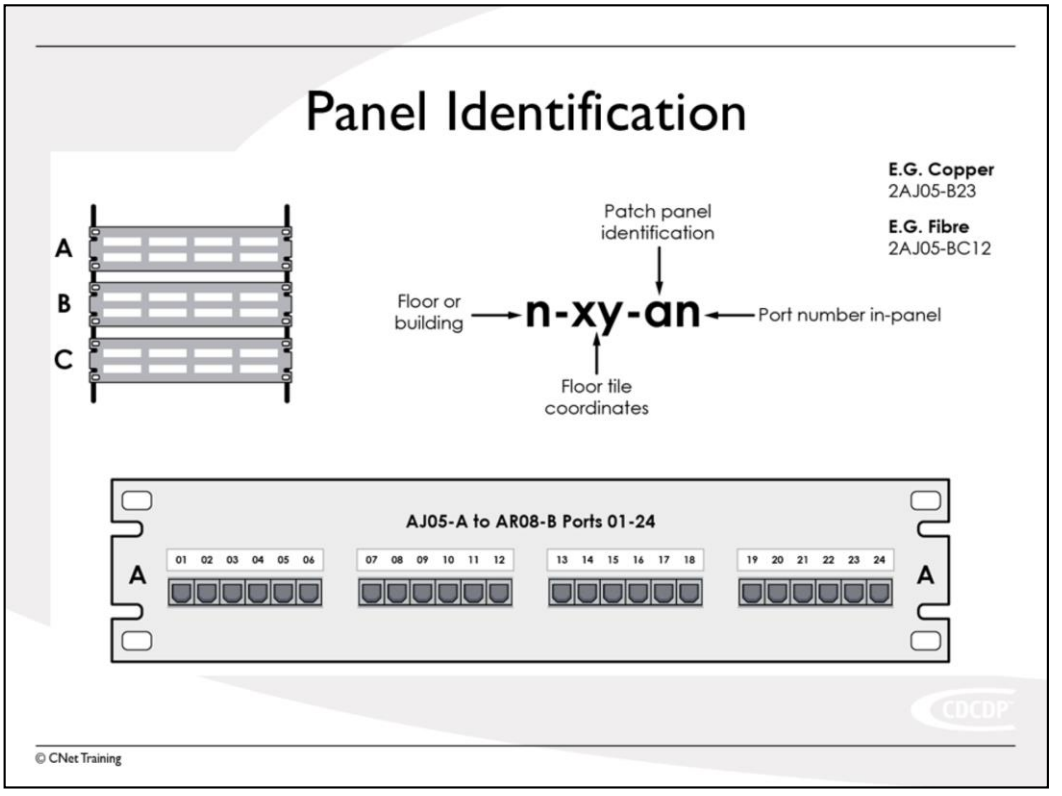
All cabling Standards reference or specify the above requirements. Each part of the network cabling infrastructure and distribution system should be uniquely identified.

The administration system will be a critical factor in the ongoing management and ownership of the Data Centre. Time and effort invested now by the CDCD is well worth it!

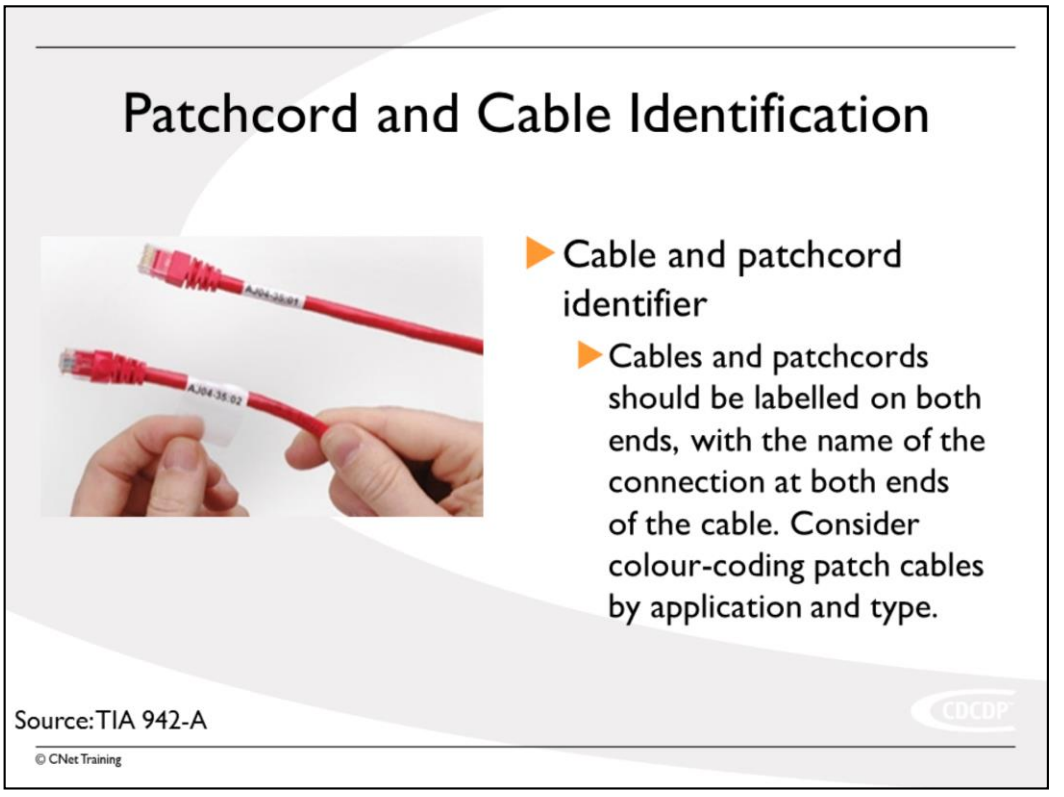
The system should be documented fully, and the CDCD should ensure it is applied, prescriptively if necessary, by all parties involved in the Data Centre build. Anarchy is the alternative!



It is also important the room's coordinates are uniquely identified. One way of doing this is to use the floor tiles as reference points, where each floor tile is identified on a grid, and the cabinet name depends on the tile where the right front corner of the cabinet is positioned. In this particular example, the green cabinet is AJ05 and the blue cabinet is AR08. This alpha-numeric system works well for medium to large Data Centre layouts. However, many Data Centre designers adopt a simple row identification format.



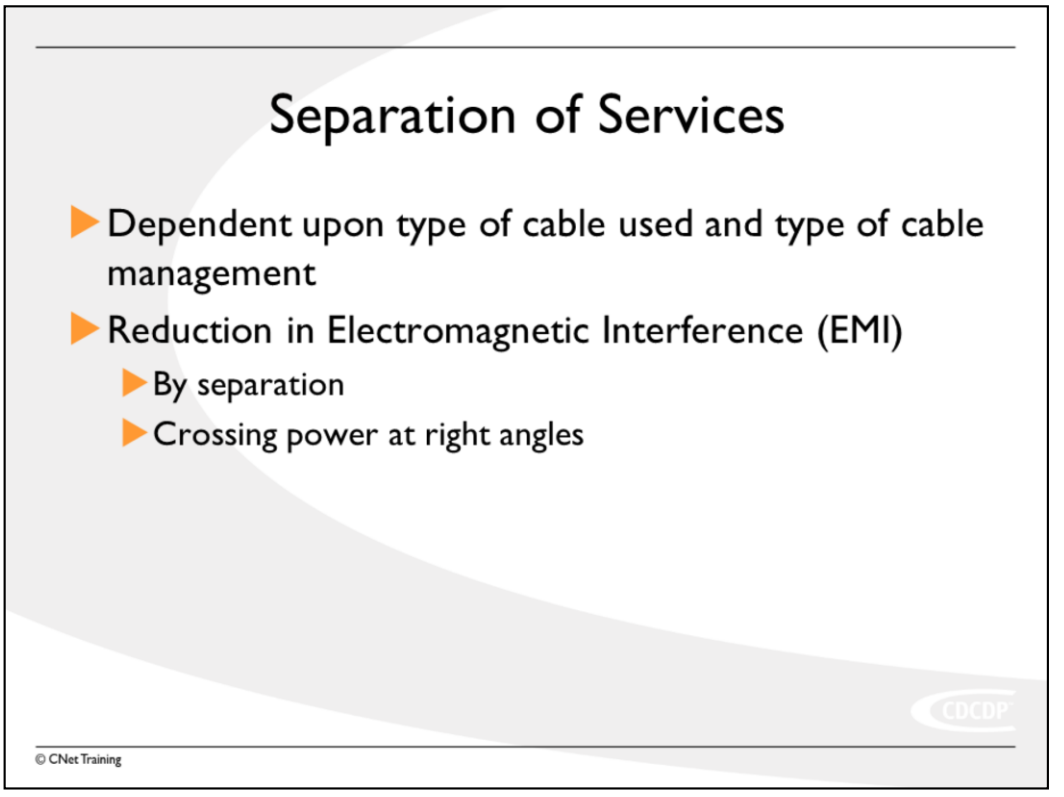
Patch panels should also be uniquely labelled.



Patch cables should be labelled. Many organisations choose not to do this, but others adopt colour schemes for patching, such as:

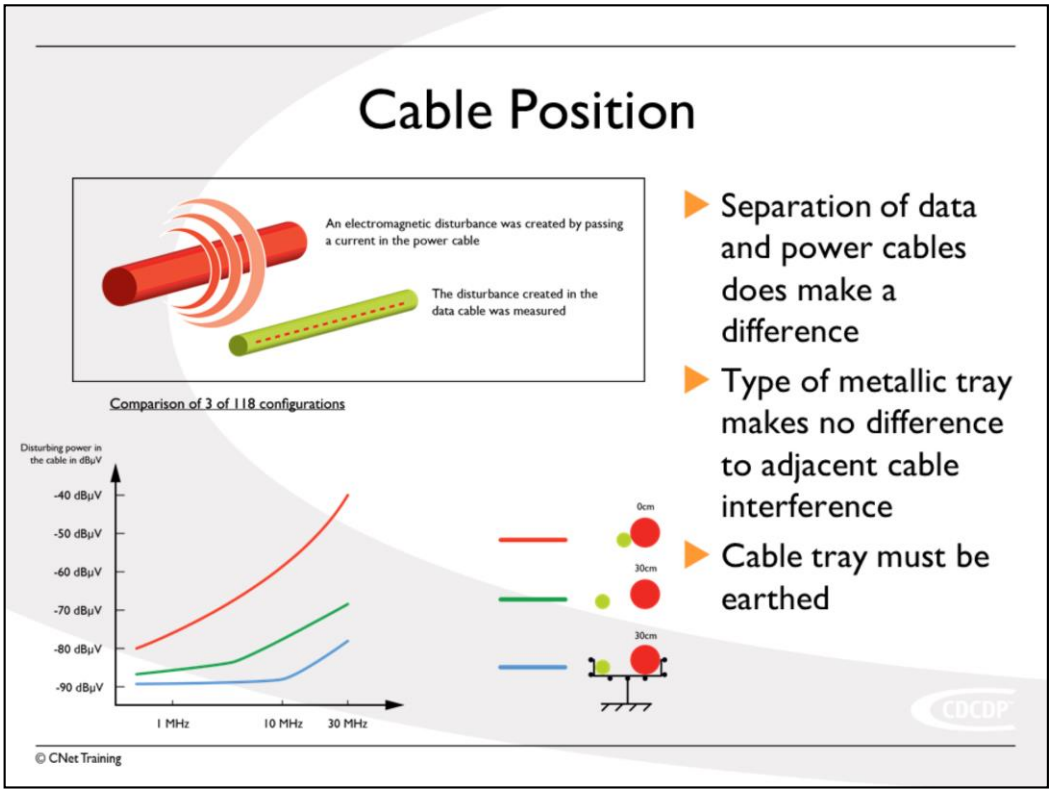
- **Black** - From servers to patch
- **Blue** - From patch to switch
- **Grey** - From switch to workstation switches/hubs
- **Yellow** - From switch to firewall/router

TIA 606-B: Administration Standard for Telecommunications Infrastructure states all labels should be machine-generated.

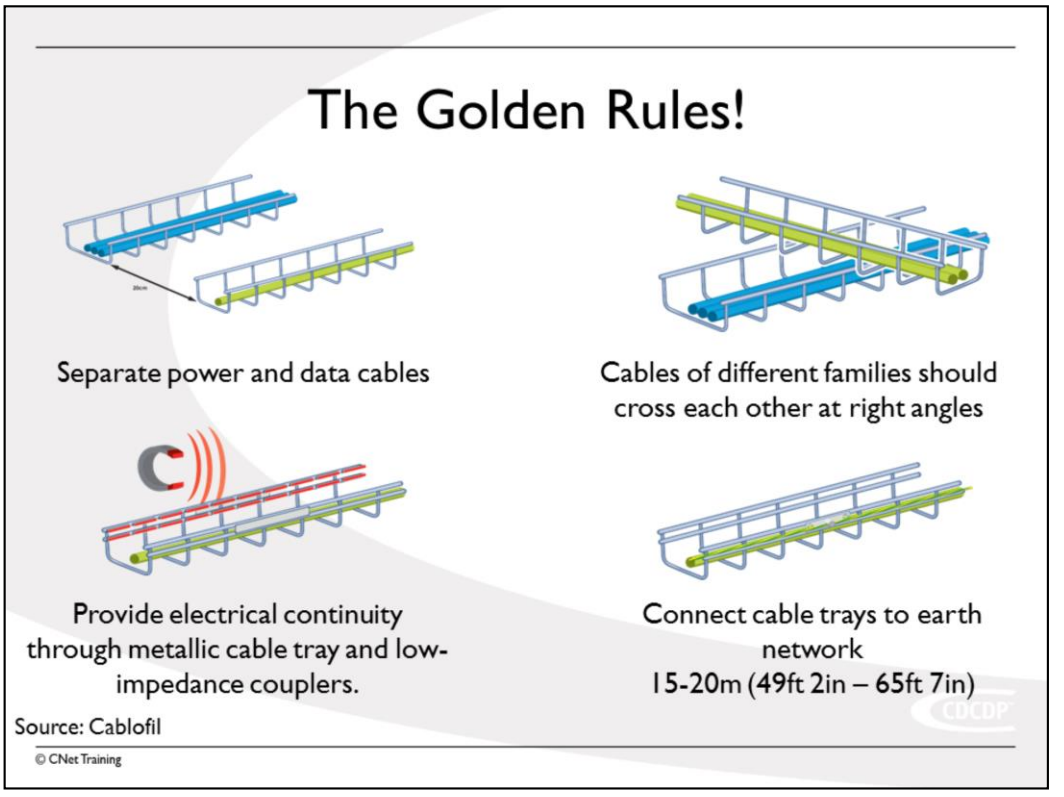


Cable routing can minimise interference from adjacent services such as mains power cables. In an ideal world, there is no reason to separate a 'balanced' data cable from a 'balanced' power cable to avoid performance issues. However, the world is not ideal and 'balance' is never perfect.

ISO, EN and TIA Standards exist for guidance. Electrical Standards and codes also apply, which may require separation for safety reasons.



Good routing can make a major difference to the data network performance. Bad routing can totally ruin it.



There are some simple things which can be done without getting too technical.

Labels shall be durably affixed. Labels shall be resistant to environmental conditions at the point of installation, such as moisture, heat or ultraviolet light - and shall have a design life equal to or greater than that of the labelled component (EN 50174).

Separation – EN 50174-2

- New guidance based on susceptibility of copper data cables, operating environment (M.I.C.E), application and volume of power cabling
  - Screened cable is less susceptible than unscreened
- Take cable classification, apply environmental conditions and containment, get separation distance, then multiply by power cable factor. This establishes the minimum recommended separation distance
- If all factors are compliant, no segregation is required other than for safety

© CNet Training

Cable routing can minimise interference from adjacent services such as mains power cables.

- **M.I.C.E** - Mechanical, Ingress Protection, Climatic and Chemical, Electromagnetic

M.I.C.E

- This concept is a formal approach by system designers to systematically classify their environments, thus helping to define the materials to build the network
- M.I.C.E is broken down to cover:
  - Mechanical: Shock, vibration, crush, impact
  - Ingress Protection: Particulate ingress, immersion
  - Climate and Chemical: Ambient temperature, humidity, liquid pollution, gaseous pollution
  - Electromagnetic: Electrostatic discharge, radiated RF, conducted RF, magnetic fields

© CNet Training

Cable Classification – EN 50174-2

Information Technology Cable			
Screened	Unscreened	Coaxial / Twinaxial	
Coupling attenuation at 30MHz to 100MHz dB	TCL at 30MHz to 100MHz dB	Screening attenuation at 30MHz to 100MHz dB	Segregation Classification
≥ 80 a	≥ 70 – 10 x lg f	≥ 85 d	d
≥ 55 b	≥ 60 – 10 x lg f	≥ 55	c
≥ 40	≥ 50 – 10 x lg f c	≥ 40	b
< 40 a	< 50 – 10 x lg f	< 40	a

a) Category 7 meets Segregation Classification 'd'.

b) Screened Category 5 & Category 6 (EN 50173-1 2007) meet Segregation Classification 'c'.
These cables may deliver performance of Segregation Classification 'd' provided that the relevant coupling attenuation requirements are also met.

c) Unscreened Category 5 & Category 6 (EN 50173-1 2007) meet Segregation Classification 'b'.
These cables may deliver performance of Segregation Classification 'c' or 'd' provided that the relevant TCL requirements are also met.

d) Category BCT-C meet Classification 'd'.

- Manufacturers must provide these data or confirm compliance

© CNet Training

Standards contain recommended minimum separation distances.

EN 50174-2 introduces a modified process for working out separation distances based on the principles of M.I.C.E.

The first consideration is the type of data cable involved, and they are categorised as shown.

Cable Environmental - EN 50174-2

		Information Technology Cable		
Segregation Classification (from Table 3)	Separation without electromagnetic barrier	Open metallic containment a	Perforated metallic containment b c	Solid metallic containment b c
d	10mm	8mm	5mm	0mm
c	50mm	38mm	25mm	0mm
b	100mm	75mm	50mm	0mm
a	300mm	225mm	150mm	0mm

a) Screening performance (0MHz to 100MHz) equivalent to welded mesh steel basket of mesh size 50mm x 100mm (excluding ldders). This screening performance is also achieved with steel tray (duct without cover) of less than 1.0mm wall thickness and more than 20% equally distributed perforated area.

b) Screening performance (0MHz ro 100MHz) equivalent to steel tray (duct without cover) of 1.0mm wall thickness and no more than 20% equally distributed perforated area. This screening performance is also achieved with screened power cables that do not meet the performance defined in Note d.

c) The upper surface of installed cables shall be at least 10mm below the top of the barrier.

d) Screening performance (0MHz to 100MHz) equivalent to a steel conduit of 1.5mm wall thickness.
Separartion specified is in addition to that provided by any divider/barrier.

- Class of cable in types of containment

© CNet Training

The next consideration is the environment surrounding the data cable, for example, the type of containment.

Number of Power Cables - EN 50174-2

Electrical Circuit Type a, b, c	Quantity of Circuits	Power cabling factor *P*
20A 230 V 1-phase	1 to 3	0.2
	4 to 6	0.4
	7 to 9	0.6
	10 to 12	0.8
	13 to 15	1.0
	16 to 30	2.0
	31 to 45	3.0
	46 to 60	4.0
	61 to 75	5.0
	> 75	6.0

a) 3-phase cables shall be treated as 3 off 1-phase cables.

b) More than 20A shall be treated as multiples of 20A.

c) Lower voltage AC or DC power supply cables shall be treated upon their current ratings i.e. a 100A 50V DC cable = 5 of 20A cables (*P*=0.4)

- Number of power cables = Multiplication factor for separation distance

© CNet Training

The number and type of interferers (power cables) has an impact which must be accounted for.

Other EMI Sources - EN 50174-2

Source of Disturbance	Minimum separation (mm)
Fluorescent Lamps	130 a
Neon Lamps	130 a
Mercury Vapour Lamps	130 a
High-intensity Discharge Lamps	130 a
Arc Welders	800 a
Frequency Induction Heating	1000 a
Hospital Equipment	b
Radio Transmitter	b
Television Transmitter	b
Radar	b

a) The minimum separations may be reduced provided that appropriate cable management systems are used or product suppliers guarantees are provided.

b) Where product suppliers guarantees do not exist, analysis shall be performed regarding possible disturbances. e.g. frequency range, harmonics, transients, bursts, transmitted power, etc.

- Electrical noise generated by different types of electrical loads must be considered

© CNet Training

Separation ISO 14763-2

- The ISO 14763-2 has now adopted M.I.C.E
  - 5.3.4.1 Requirements:
    - The technical specification shall detail the intended installation and operational environment conditions. The M.I.C.E classification system described in ISO/IEC TR 29106 shall be used where the intended installation and operational environmental conditions lie within the boundaries detailed by M.I.C.E

© CNet Training

The move towards harmonisation continues.

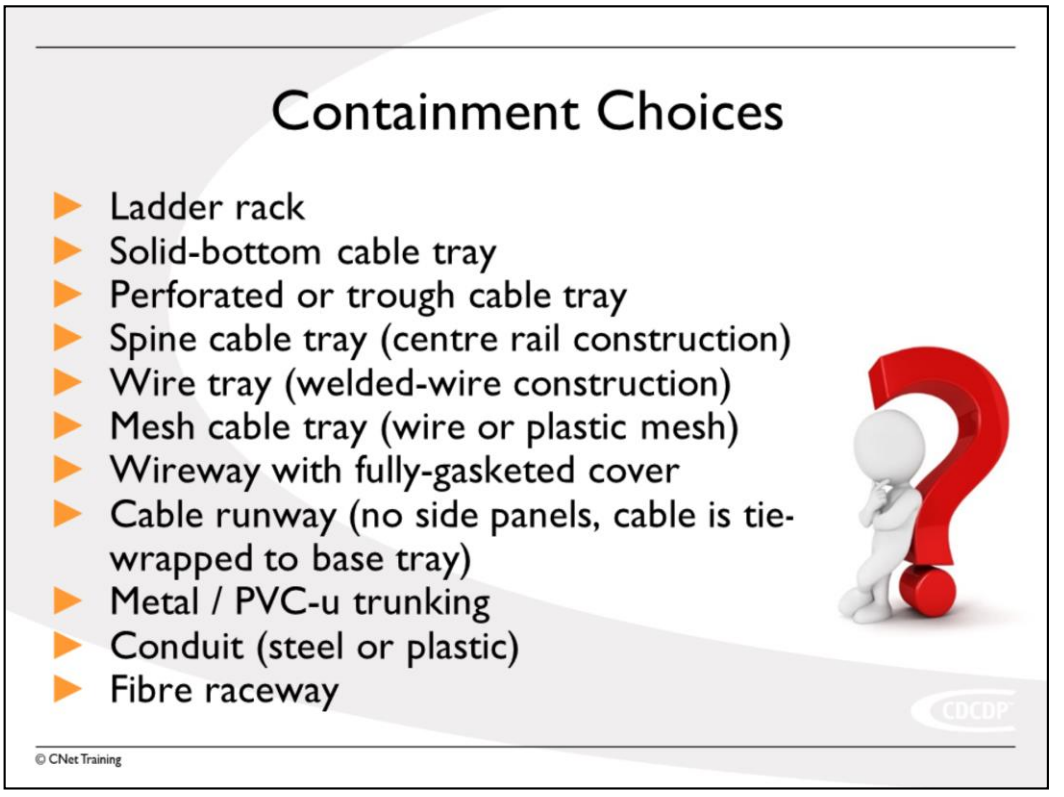
Separation NECA-BICSI

Minimum separation distances from possible sources of EMI exceeding 5kVA	
Condition	Minimum Separation Distance
Unshielded power lines or electrical equipment in proximity to open or non-metal pathways.	610mm (24in)
Unshielded power lines or electrical equipment in proximity to a grounded metal conduit pathway.	300mm (12in)
Power lines enclosed in a grounded metal conduit (or equivalent sheilding) in proximity to a grounded metal conduit pathway.	150mm (6in)
Electrical motors and transformers.	1200mm (47in)

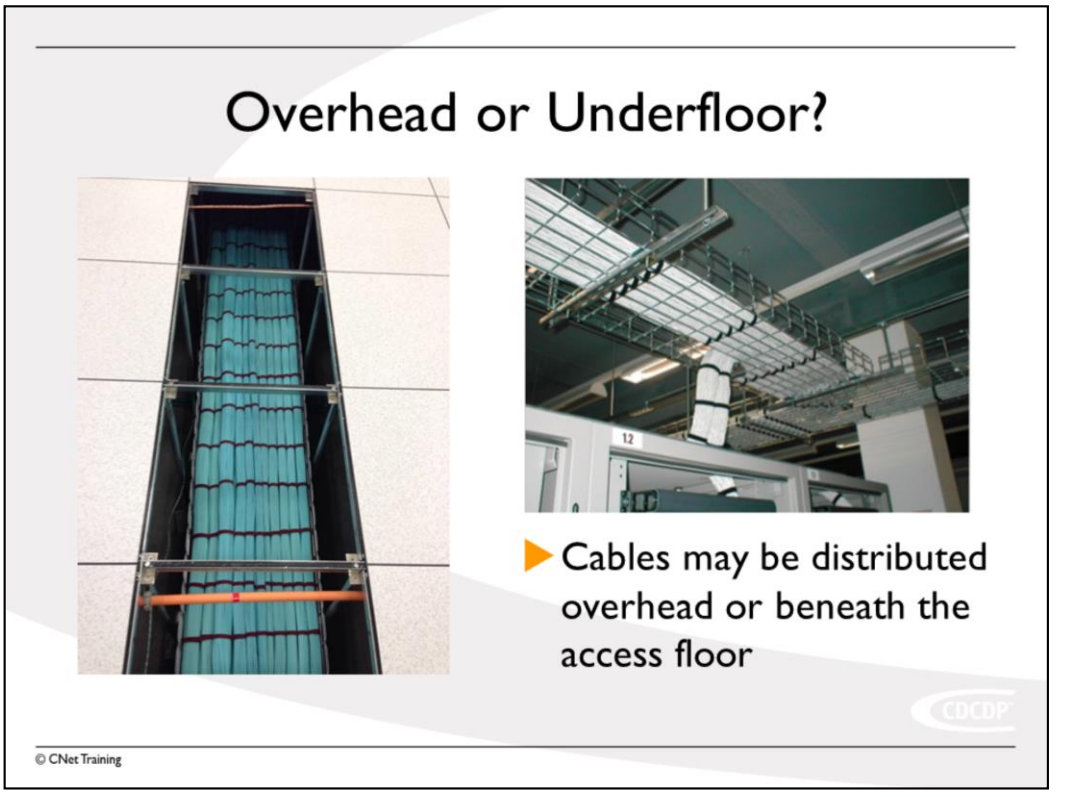
- For branch circuits of 5kVA or less, no additional separation should be necessary

© CNet Training

For unusual situations when excessive noise is present on branch circuits, see TIA 569-B, Annex C - Noise reduction guidelines.



Cables can be supported and routed by a range of containment methods; several of these are often found together in the same installation.



Cables can be distributed overhead or under the raised floor. Sometimes data cables are routed overhead and the power cables under floor, or vice versa.

Overhead or Underfloor?

Implementation	Positives	Negatives
Overhead	• Less expensive construction • Easier to add cabling • Easier to trace cabling • Does not constrict airflow • Separates data cabling from high voltage (under-floor) cabling • May provide a "technology showcase" for the cabling solution	• Must be designed around different cabinet heights • Must be designed around ceiling fixtures, such as sprinkler systems • Requires ladders or platforms for MAC work, potential safety issue
Raised Floor	• "Clean" Data Centre appearance • More secure, cabling pathways are not exposed	• May block under-floor airflow, driving up HVAC costs • Limited room for cabling • Higher building costs • Disruption of airflow and pressure during MAC work • Open floor tiles may be safety issue

- All factors a CDCD must properly consider prior to installing containment

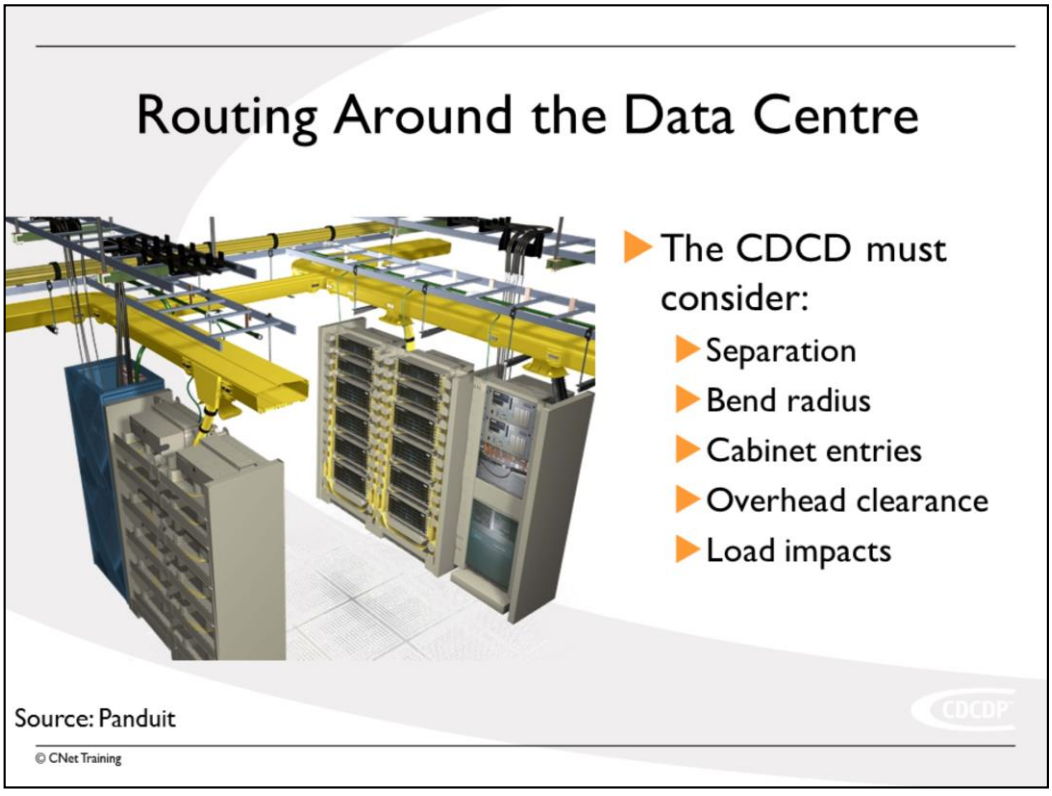
© CNet Training

Access to Overhead Cable Trays

- In Data Centres that use overhead cable trays, the normal separation distances provided by Standard practices provide adequate access
- As specified in ANSI/TIA-569-C, a minimum of 300mm (12in) access headroom between the top of a tray or runway and the bottom of the tray or runway above shall be provided and maintained

© CNet Training

Cables can be routed overhead. If so, it is necessary to allow sufficient vertical clearance between different cable runs.



Designing the cable routing around the Data Centre is very important. It is equally important to consider how the cables will enter the equipment racks. Items such as separation and bend radii must still be remembered by the CDCD.

Fill Factors

Length between supports (mm)	Cable Stack Height (mm)
100	140
150	136
250	128
500	111
750	98
1000	88
1500	73

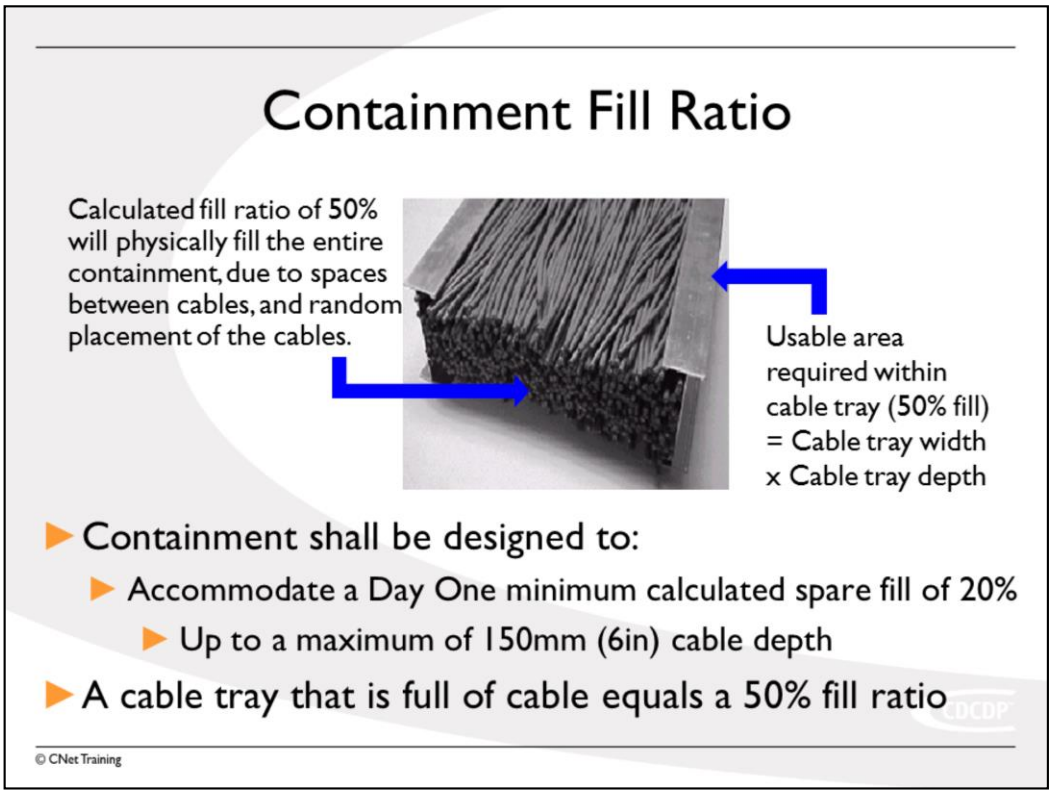
- Ratio of the Cross Sectional Area (CSA) of cables (including sheath) to the internal CSA of the containment
- 50% fill factor = Full
- Spare capacity recommendation = 20%
- Maximum cable stack height = 150mm (6 in)
- Basket, ladder, J-hooks, etc.

© CNet Training

If cable trays, trunking and conduit are used, there are recommendations on how many cables they can contain. There are tables and equations covering this calculation, which the CDCD can employ.

A good rule of thumb is to work to a 40-50% fill, unless a manufacturer's recommendations are available.

The maximum height of the cable stack is 150mm (6 in). Anything beyond will risk deforming the cables at the bottom.



Cable trays, basket, ladder racking and other containment shall be designed to allow room for future expansion, and for addition and removal of cables once the Data Centre becomes operational.

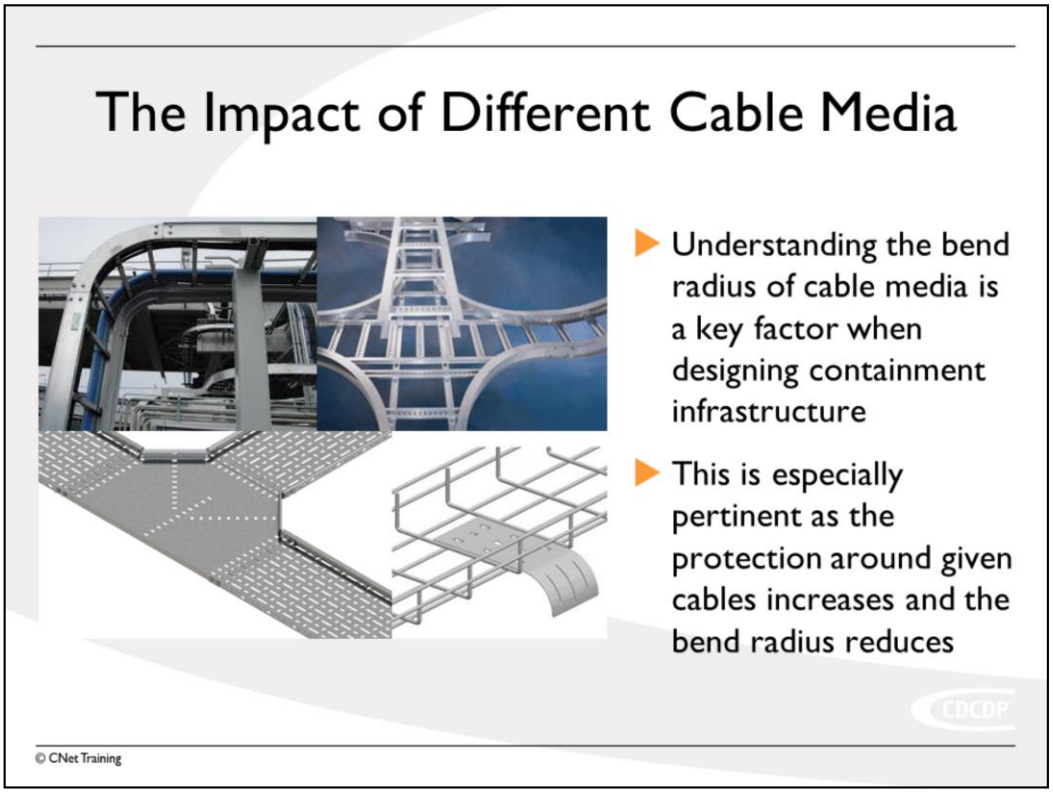
A calculated fill ratio of 50% will physically fill the entire containment, due to spaces between cables, and random placement of the cables.

For example, what is the minimum width of a 75mm deep cable tray supporting 1000 cables, each with a diameter of 5.5mm?

- Area of one cable = $(\textit{Cable diameter})^2 \times \pi / 4$
- Area of one cable $=(5.5)^2 \times 3.14 / 4 = 23.75\text{mm}^2$
- **Area of 1,000 cables = $(5.5)^2 \times 3.14) \times 1000 / 4 = 23{,}746\text{mm}^2$**

Multiply this occupied area by 1.2 to give 20% oversize for Day Two expansion

- Usable area or area required within cable tray (50% fill) = Cable tray width x Cable tray depth / 2
- 1,000 cables = $(23{,}746\text{mm}^2) \times 1.2$ = Cable tray width *x* 75mm / 2
- Minimum width of cable tray = **759.9mm**



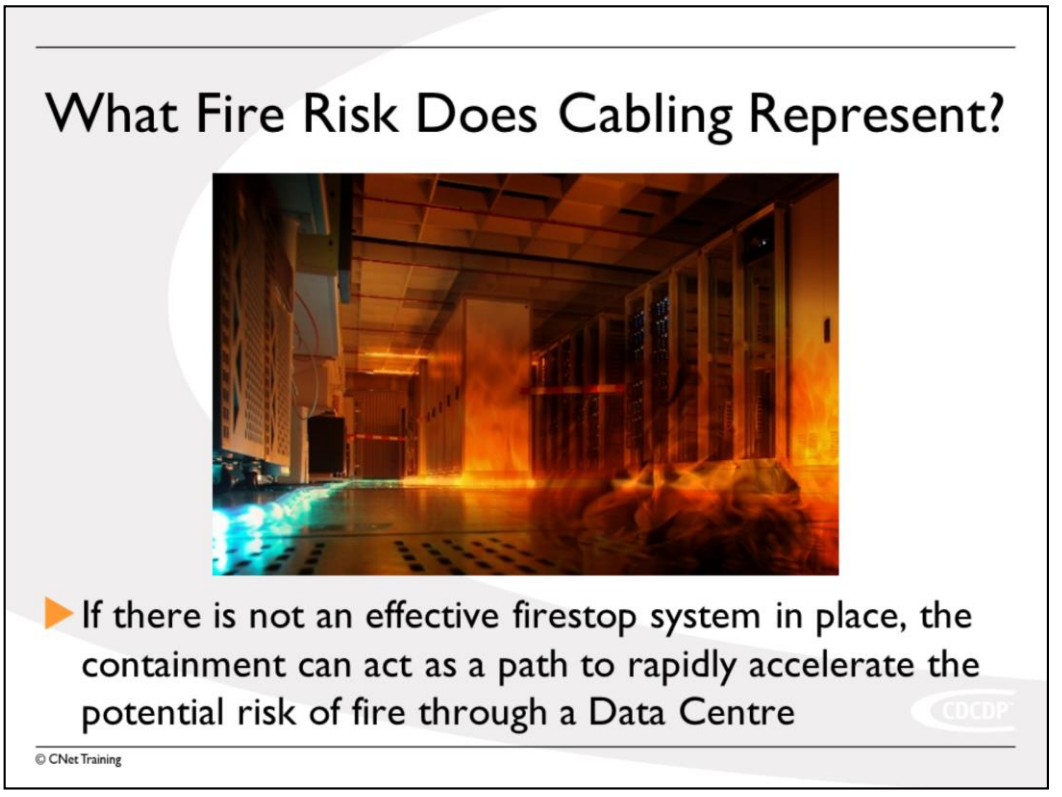
Minimum bend radii must be observed throughout the whole cable route in order to ensure the design performance of the cable is not impaired. EN 50174-2 states the minimum bend radius is specified by a manufacturer's instructions. If instructions do not exist, the following shall apply:

- The minimum bend radius for 4-pair balanced cables shall be eight times the cable diameter
- The minimum bend radius for optical fibre cables and coaxial cables shall be ten times the cable diameter
- The minimum bend radius for other metallic information technology cables shall be eight times the cable diameter

Cabling Exiting Containment

- TIA 942-A states:
  - There shall be a minimum of 20mm (0.75in) from the bottom of the access floor tiles to the top of the cable tray
- Equal considerations should be undertaken for overhead cables exiting the containment to the top of the cabinet

© CNet Training



The potential risk of fire escalation in a Data Centre can be directly aligned to the cable type, and pathways or containment within the environment, especially if there is no (or ineffective) firestopping.

It is key the CDCD understands the characteristics of structured wire cables, and how they are viewed and installed within given regions. In the USA, plenum grade cables are extensively used, which burn very slowly, but give off smoke and poisonous gas. Low-smoke, zero halogen (LSZH) cable is used extensively in the UK and Europe. Under fire conditions, it does not give off thick smoke or poisonous gases, but burns fiercely.

Building Regulations, Part B: Firestopping

- **11.12** In addition to any other provisions in this document for firestopping:
  - a. Joints between fire-separating elements should be firestopped
  - b. **All openings** for pipes, ducts, conduits or cables to pass through any part of a fire-separating element **should be**:
    - i. Kept as few in number as possible
    - ii. Kept as small as practicable
    - iii. Firestopped (which in the case of a pipe or duct, should allow thermal movement)
- The CDCD must understand the local fire regulations

© CNet Training

The CDCD must ensure fire regulation requirements are built into the cable routing design. All country-specific local building regulations will have a similar requirement.

Firestopping through wall cable penetrations involves more than simply purchasing and installing an appropriate product. A firestopping system must incorporate the fire-rated wall, the penetration, cable containment and cabling that passes through that given penetration. Ideally, it should be a warranted system that is checked and maintained on a regular basis.

Firestopping systems can be versatile and come in various intumescent applications:

- Caulk
- Putty sticks and stop mortar
- Firestop blocks
- Firestop pillows
- Mechanical collars

The CDCD must be aware of the fire resistance rating of products in given environments. Ideally, the firestopping system should be installed by professionals, with all details recorded and regularly maintained. Some countries have specific requirements in line with local and national building codes.

Firestopping

- Only use certified products
- Installed by a certified professional
- Warranted system
- All penetrations labelled and details recorded
- Periodic maintenance programme

© CNet Training

Organise Cables in Vertical Risers, including Firestopping

- Routing in the riser and ensuring firestopping can be a challenge
- Ensure working access is considered within the design
- Ensure a routine maintenance programme is enforced

© CNet Training

Putting It Together

- Select the right cable containment for the job
- Earth / bond / ground correctly
- Label pathways
- Label cables at both ends
- Understand the containment fill ratio
- Protect bend radii of copper data and fibre cables
- Maintain separation from power cables
- Keep integrity of fire barriers

© CNet Training

In summary, the CDCD must consider all the respective design aspects when deciding the cable routing.

Review

- Can you?
  - Understand the use of containment for good cable management, administration, protection and safety
  - Describe the different containment systems in use
  - State the separation distances between different services

© CNet Training

Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®) Core Unit

Delivering the IT Strategy

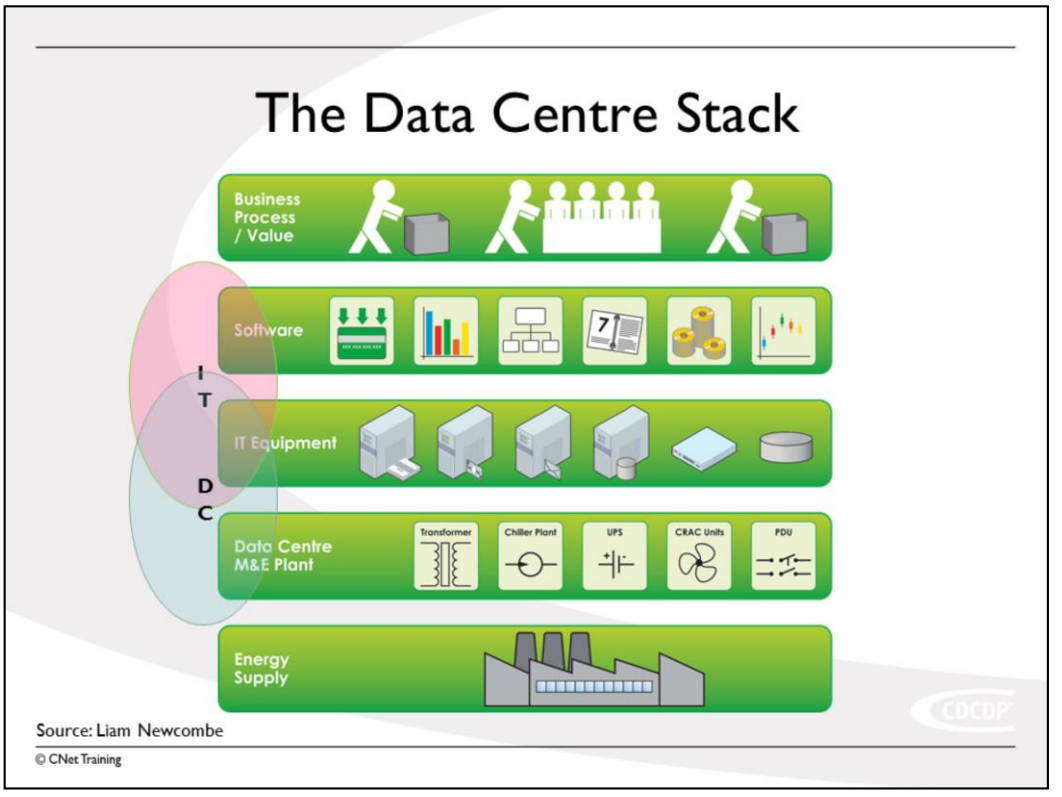
Version 1509

CDCDP

Objectives

- At the end of this module you will be able to:
  - Understand the tight link between IT strategy and the Data Centre
  - Identify network topology options
  - Explain connectivity options
  - Discuss IT Subsystems

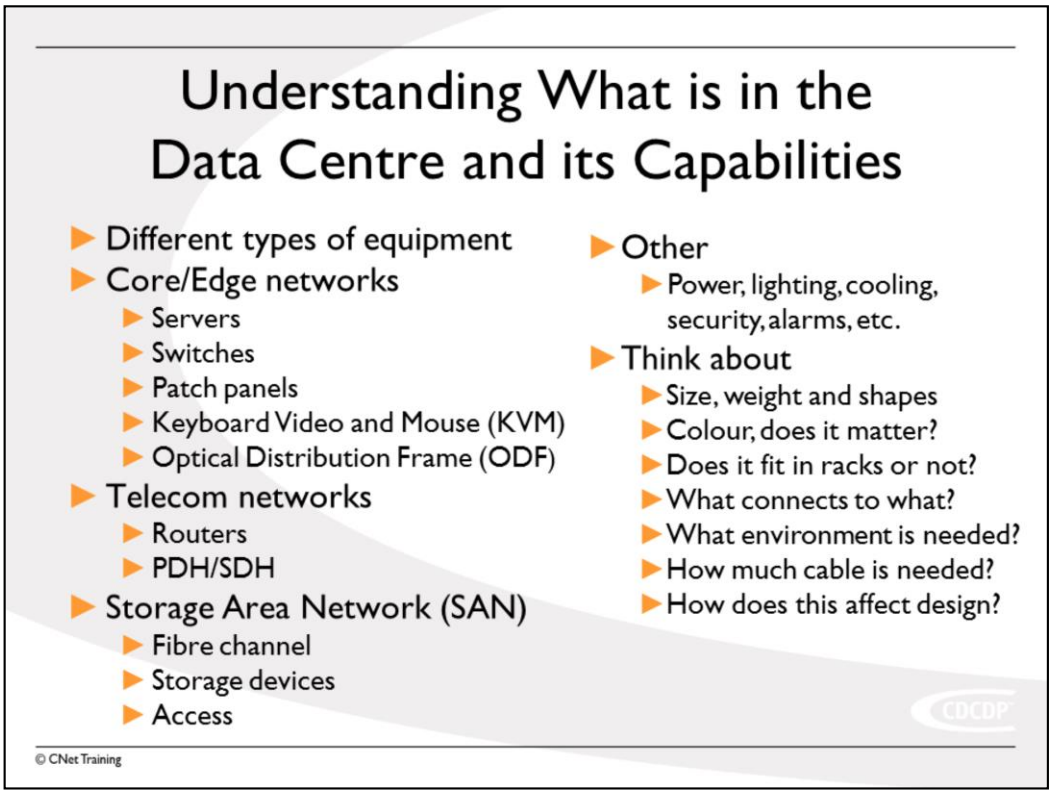
© CNet Training



Let's remind ourselves of what Data Centres are trying to achieve: We start by sourcing energy from a supplier. This energy is then delivered through the M&E plant to the IT equipment. This runs the application software that supports the business activities the Data Centre is there for.

The IT strategy must support the business, and the Data Centre needs to be able to support the IT strategy. Therefore, it is imperative the CDCD understands the requirements of the IT strategy in order to design the space. This is obviously a critical factor in the connectivity design.

Unfortunately, this is often not well-defined at the Data Centre design stage (typically two years before it goes live) and the designer must therefore build flexibility into the design to cater for a range of possible final requirements.



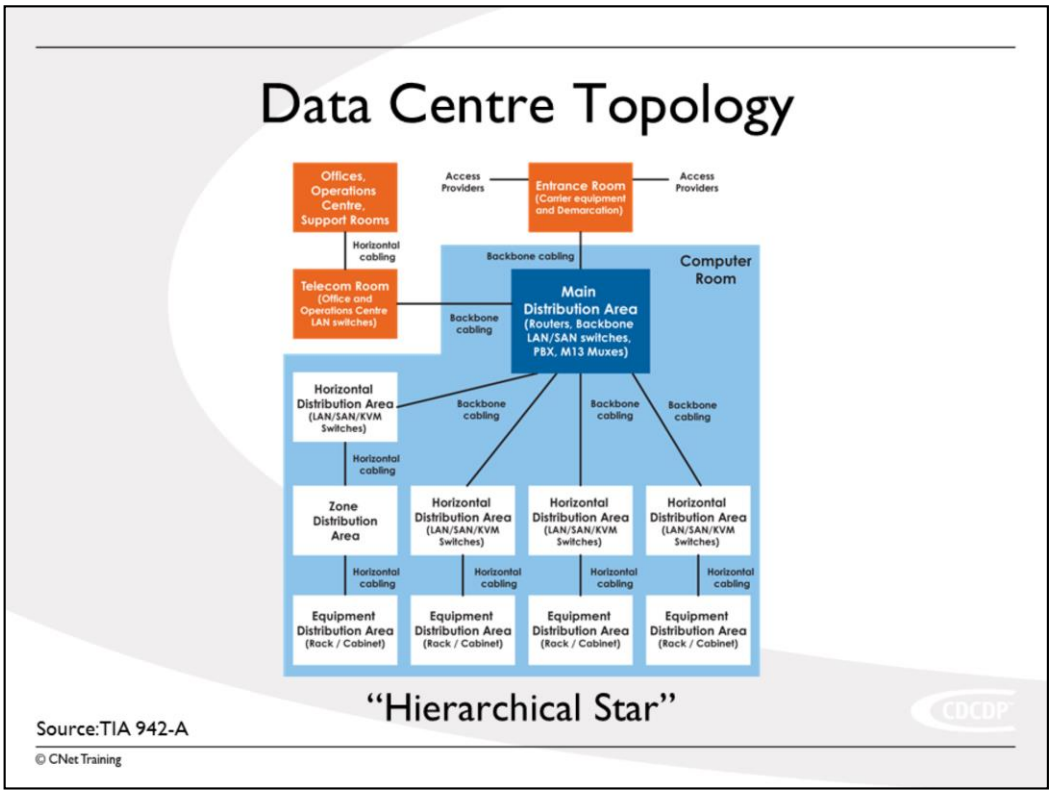
There are many different types of equipment found in a large Data Centre and the CDCD must be aware of all of them, including their delivery capabilities.

The Data Centre can be thought of in many ways, but it is useful to consider the critical IT equipment in three broad environments:

- Core/edge networks providing interconnection between the servers, storage devices, local users, etc.
- Telecom networks providing links to the outside world via Wide Area Network (WAN) technologies.
- Storage Area Networks (SAN) providing high-speed, high-capacity, secure resources for the storage and retrieval of large amounts of data.

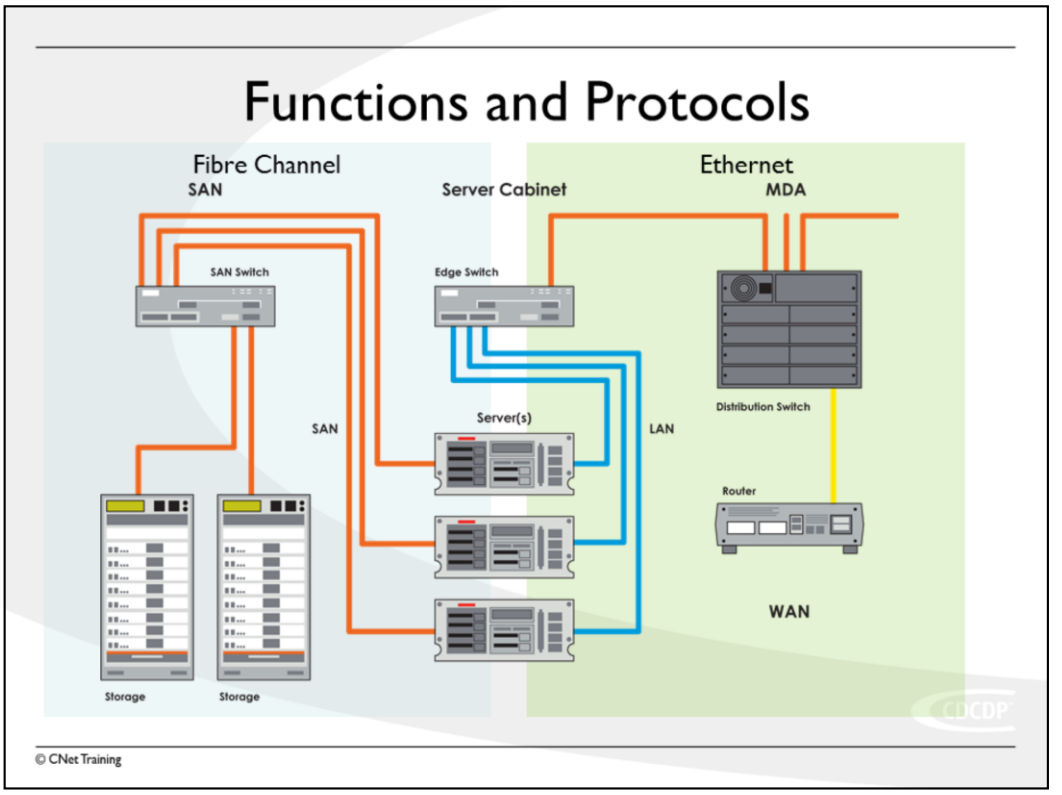
Besides the critical equipment, there is a multitude of support systems, each with its own operating requirements. The CDCD must consider these diverse environments when allocating space, power, cooling, connectivity, etc. in the computer room.

- **PDH** - Plesiochronous Digital Hierarchy
- **SDH** - Synchronous Digital Hierarchy



TIA 942-A defines the physical spaces found in a Data Centre and some of the interconnections between them.

<u>Note:</u> For a distribution system with multiple entrance rooms (i.e. Tier III and IV Data Centres), the topology can include an Intermediate Distribution Area (IDA) between the Main Distribution Area (MDA) and Horizontal Distribution Area (HDA). This is referred to as the 'Hierarchical Star' and is at present the preferred Data Centre topology.



It is easy to think everything in a Data Centre is similar, but this can catch out the unwary designer.

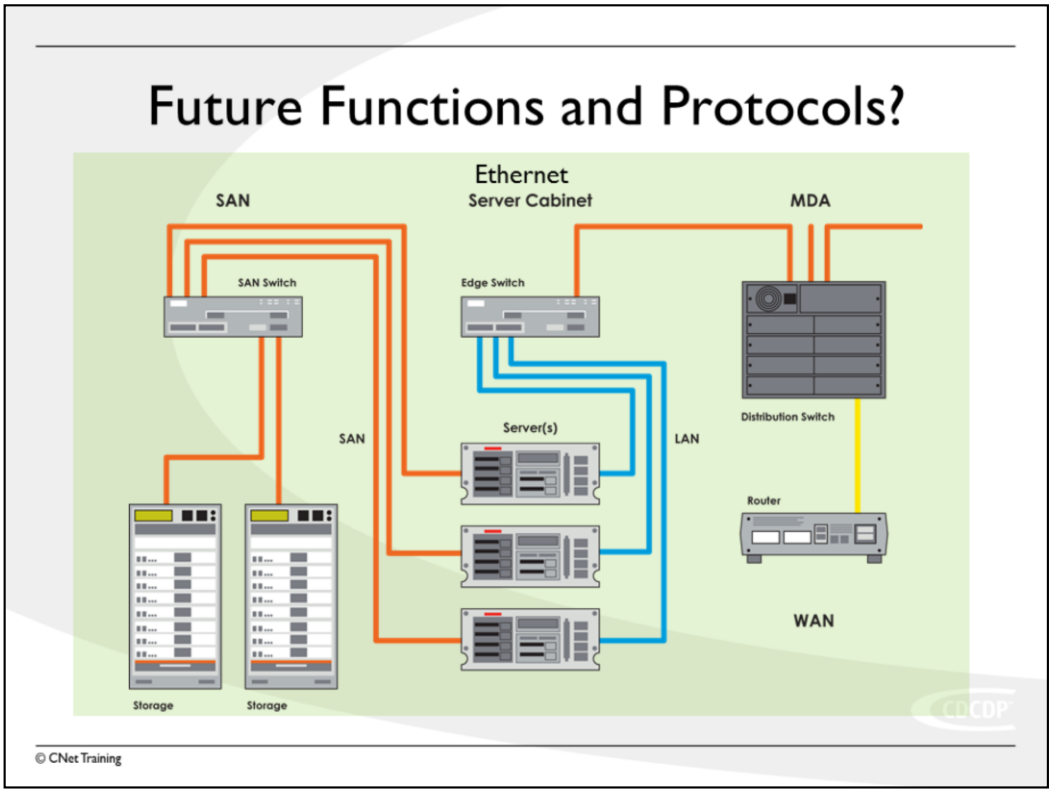
The shape, size, weight, power requirements, function, environment, etc., of equipment can vary quite dramatically, for instance:

- Servers and Local Area Network (LAN) switches generally fit into standard racks, which can be arranged in rows. Can the same be said for SAN devices? Be careful, as this can affect the layout.
- The LAN environment is Ethernet. The SAN may be Fibre Channel. How may this impact our design?
- The SAN may have different storage devices, disks, tapes, etc. What are the environmental requirements?

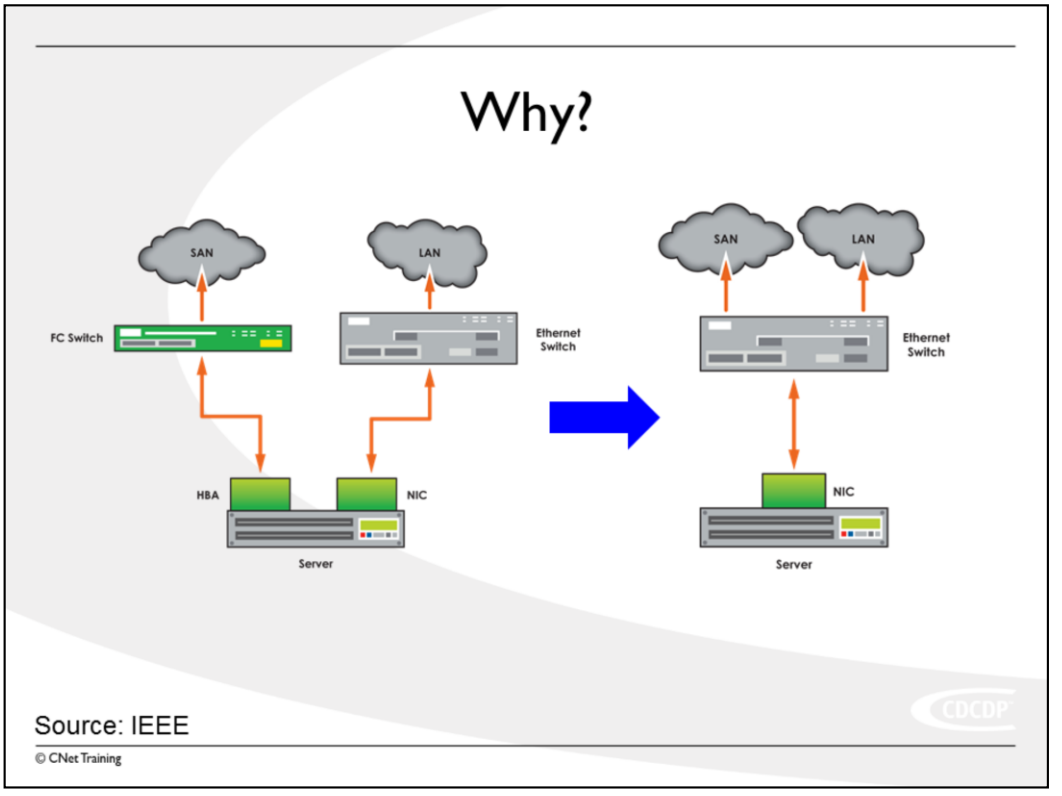
A small data environment would use direct connection between equipment, probably via main distribution frame (MDF).

A large Data Centre provides the same functionality, but on a much more complex scale - different parts of the network may be in separate rooms.

There are two common protocols used in Data Centres: Ethernet in the LAN and Fibre Channel in the SAN. Each have their own requirements and capabilities, which the CDCD must take into account.



There is work going on now which may see Ethernet become the standard bearer for the entire Data Centre. Although this has not happened yet (neither is the outcome predetermined), increasingly higher speed requirements will impact connectivity architecture.



A standard bearer for the entire Data Centre?

Ethernet-based design reduces the number of networking components, and possibly makes network management easier. However, it relies on effective operation at very high speeds.

Where?

- Bandwidth requirements for computing and core networking applications are growing at different rates
  - Servers, high performance computing clusters, blade servers, SANs and network-attached storage all currently make use of 1G and 10G Ethernet; use of 10G has significantly grown since 2008
  - I/O bandwidth projections for server and computing applications, including server traffic aggregation, indicate there will be a significant market potential for a 40G Ethernet
- Core networking applications have demonstrated the need for bandwidth beyond projected requirements for computing applications
  - Switching, routing and aggregation in Data Centres, Internet exchanges and service provider peering points, as well as high-bandwidth applications like video on demand (VOD) and high-performance computing, need a 100G Ethernet interface

Source: IEEE 802.3ba Task Force

© CNet Training

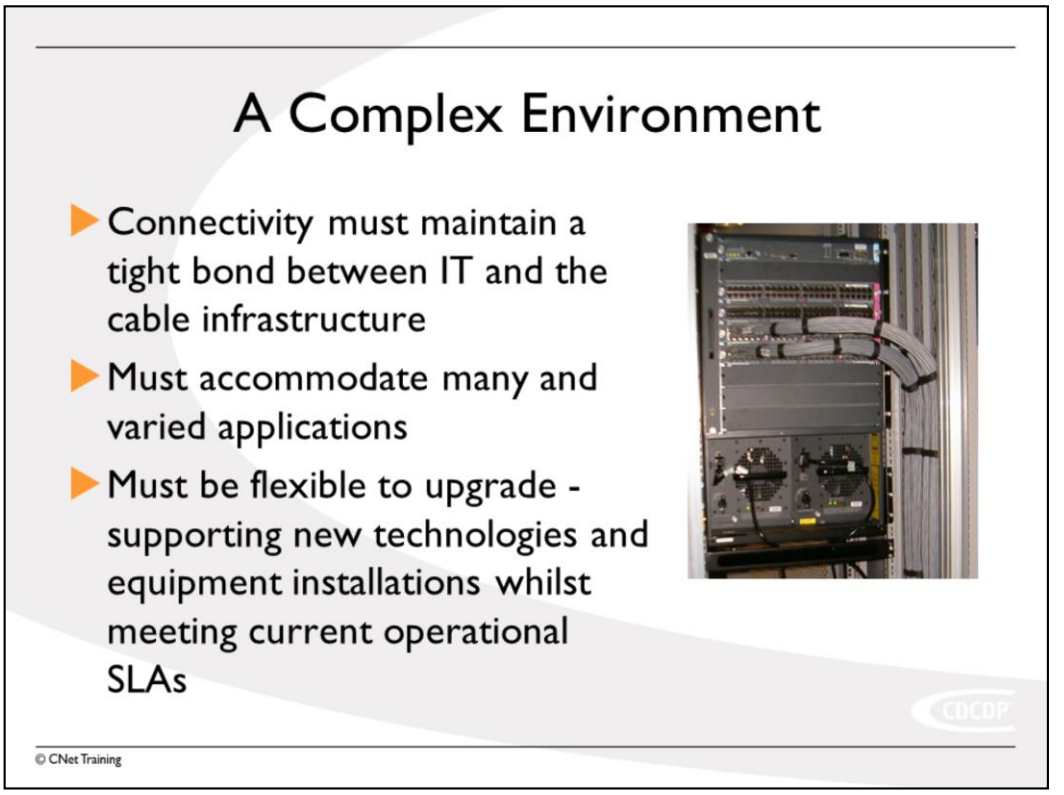
As a CDCD, it is essential the IT Strategy and projected bandwidth demands are properly evaluated and understood.

Perceived Problems?

- A key point when migrating from 10G to 40/100G Ethernet is the need to ensure precise clocking synchronisation between systems
  - Imprecise clocking between systems at 40/100G — even at 10G — can increase latency and packet loss
  - The smallest difference in the clocks between ports can cause high latency and packet loss. At 40G, it's an order of magnitude more important than it is for 10G and 1G
- This is a critical requirement in Data Centres
  - A big challenge is readying the cabling infrastructure for 40/100G
  - Ensuring the appropriate grade and length of fibre is essential to smooth, seamless operation
  - Data Centres will likely need to have parallel fibre capability

Source: Spirent Communications

© CNet Training



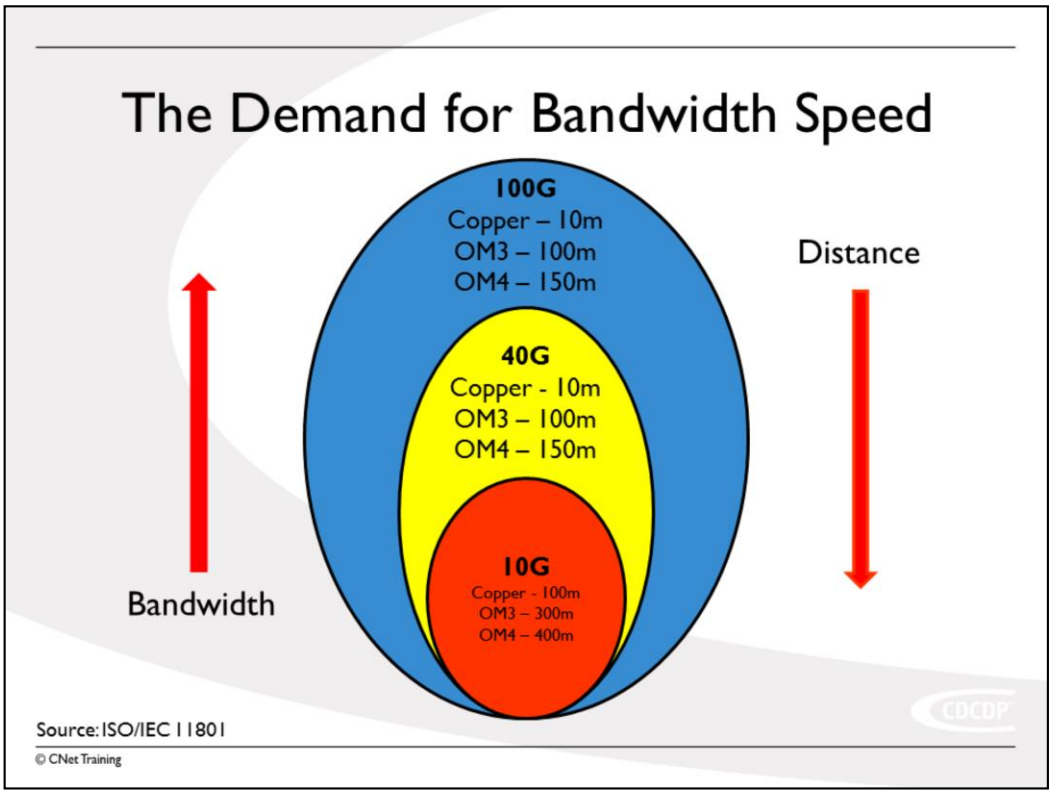
A Data Centre provides infrastructure for a wide range of IT systems, each having their own requirements. The ability of the Data Centre to meet these needs is inexorably linked to the infrastructure design from Day One.

This is made more difficult by the fact that new developments may exceed Day One requirements; the designer must ensure the plan is flexible enough to adapt to new challenges as they arise. As an example, emerging 40G and 100G Ethernet Standards support distances of 100m (328ft on OM3 multimode fibre - this is different to the 300m / 984ft capability for 10G Ethernet). The CDCD needs to consider whether this is a requirement, then incorporate it in the design.

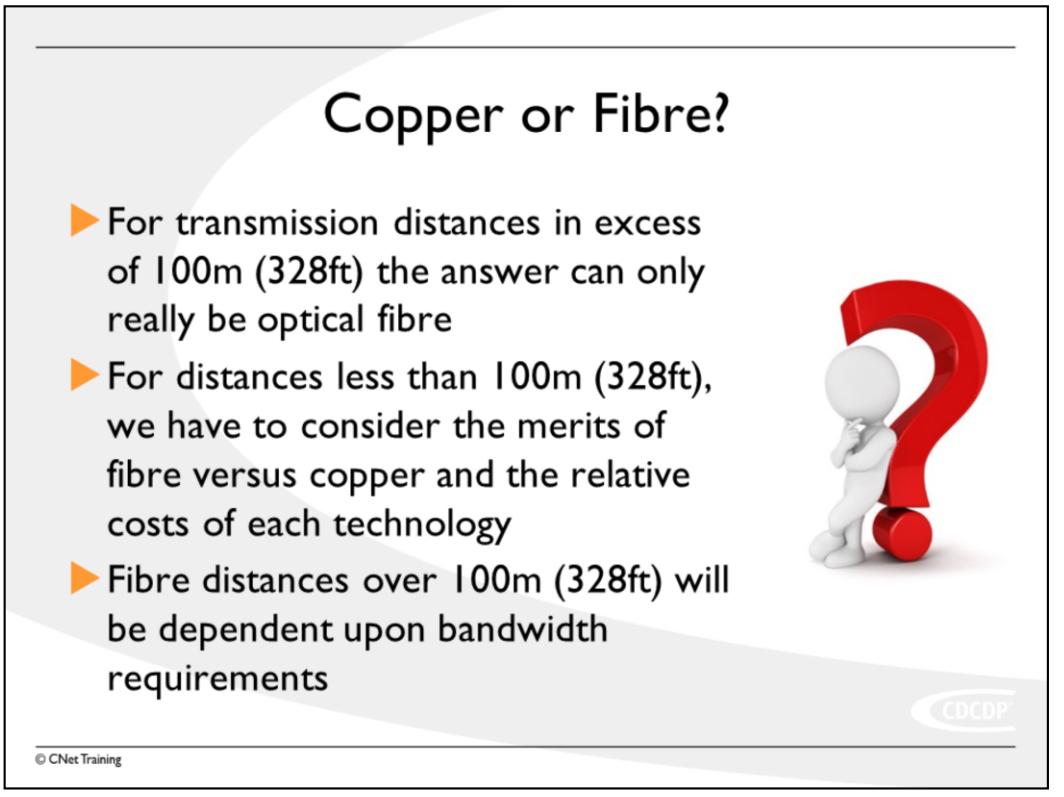
How can he/she do that?

Options include:

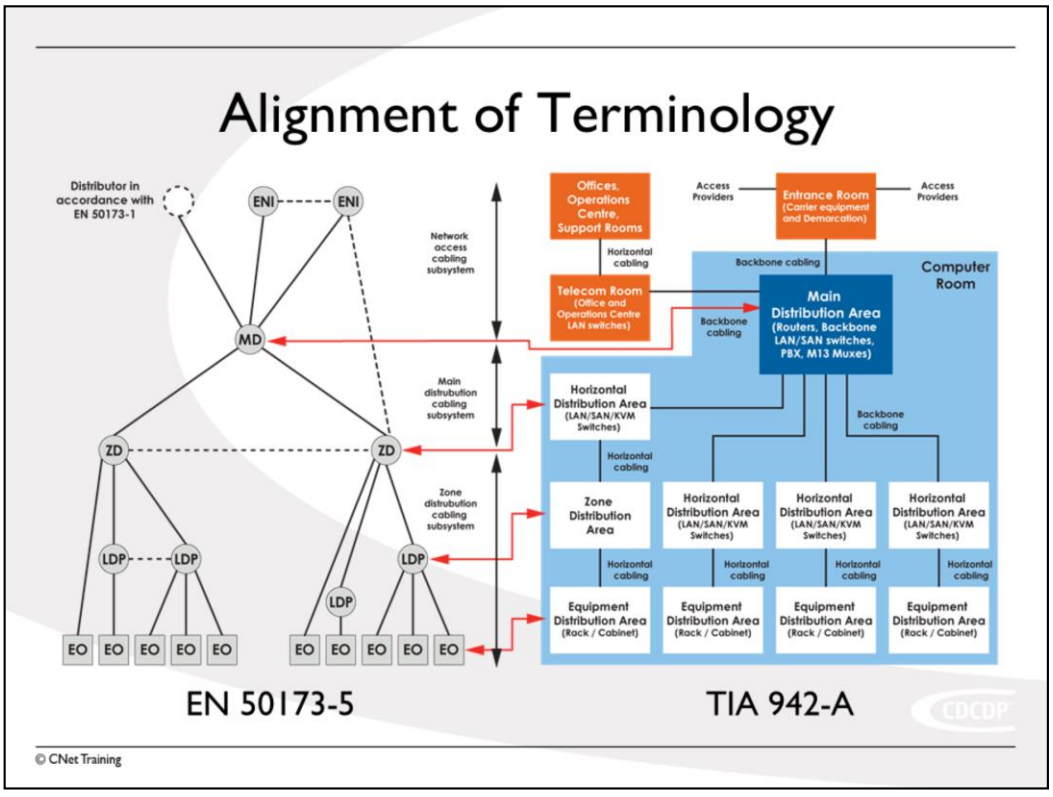
- Design the IT cabinet layout to keep all relevant equipment within the 100m (328ft) reach of OM3.
- Install a system where OM3 can be used initially, then easily replaced with singlemode fibre when 40G or 100G become a requirement.



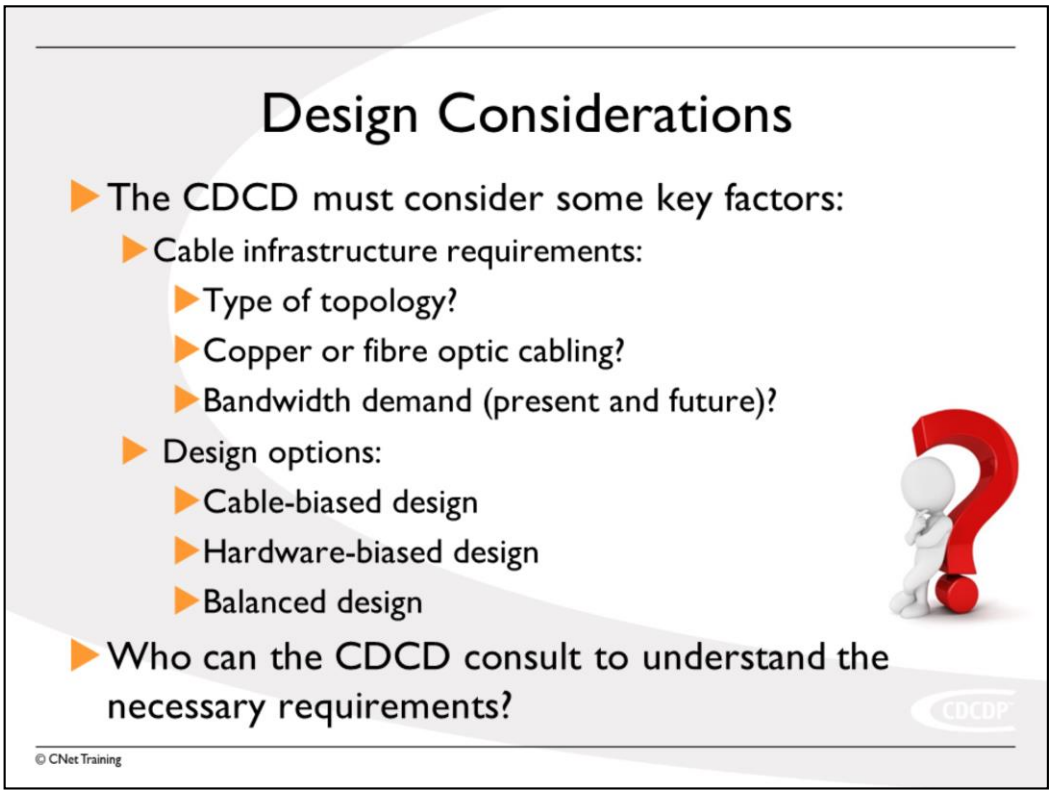
Copper cables reach their 10G limit at around 100m (328ft). Beyond that, optical fibre is needed. That said, even with multimode fibre, the distance capability will reduce in proportion to the bandwidth increase. This is a key factor that must be understood during the design phase in accordance with bandwidth and growth projections.



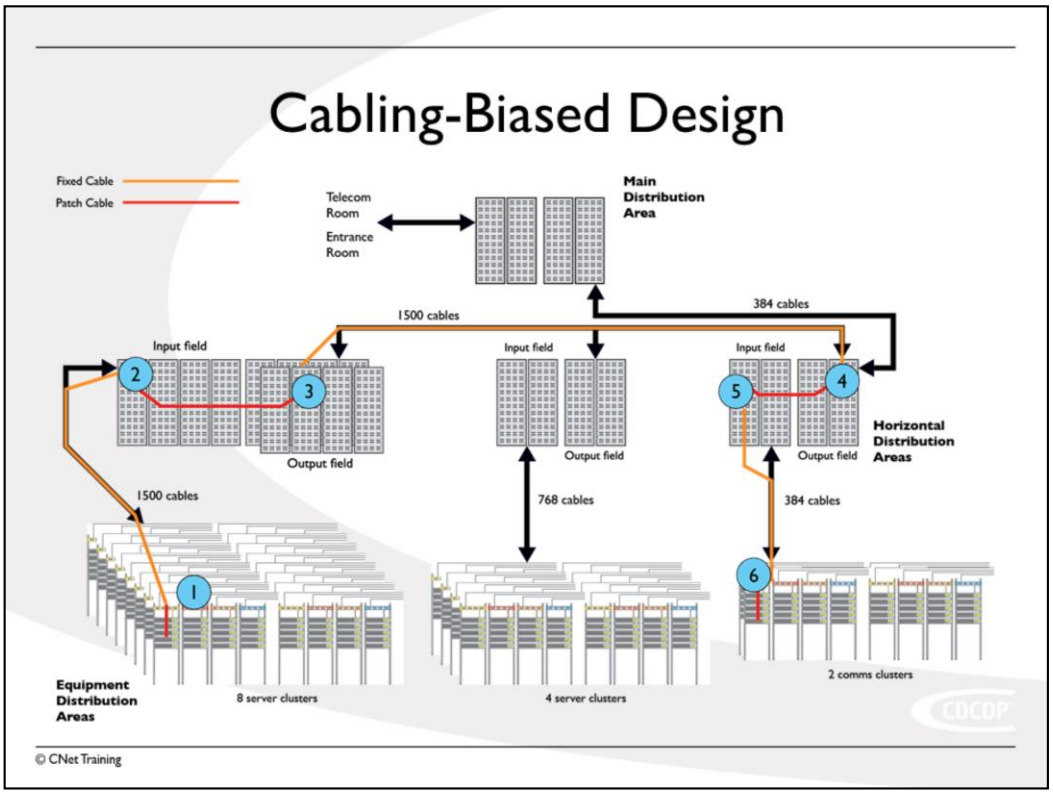
The choice between copper and fibre cable infrastructures is only relevant at short distances (100m or less) within the Data Centre environment.



The ISO and TIA Standards use different terminology, so the CDCD needs to be aware how they align.

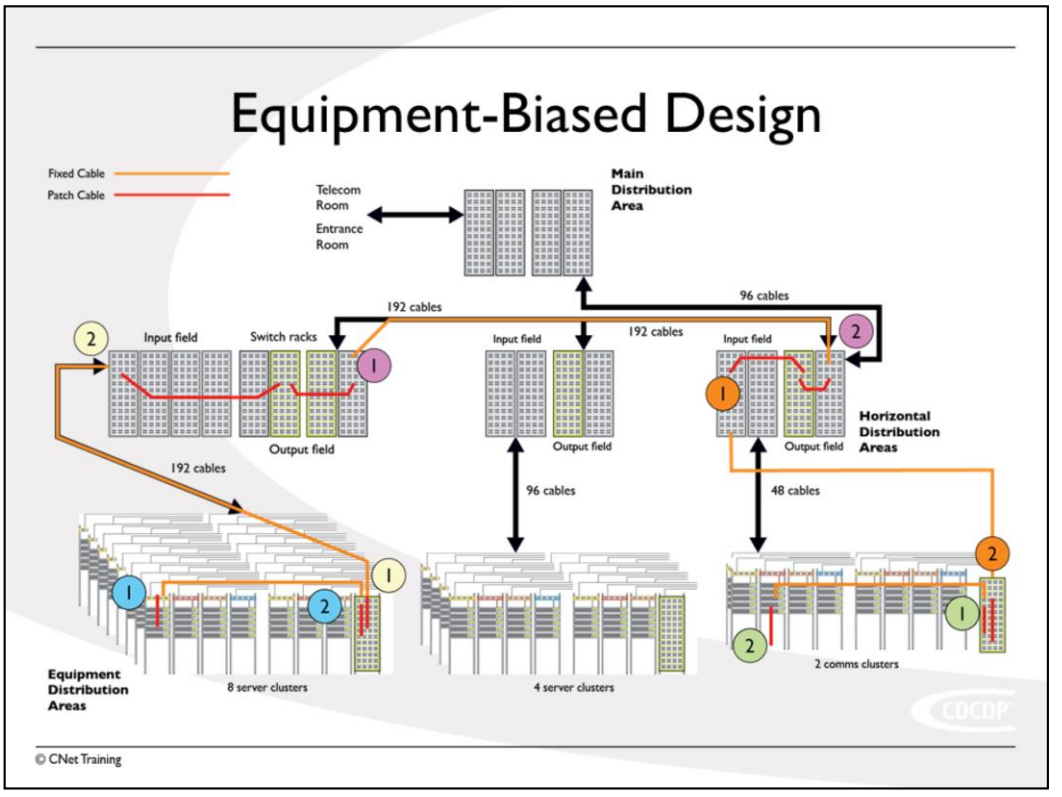


The CDCD needs to ensure a flexible design is implemented to meet both present and future IT demands. This can be a real challenge with continual advances in technology and subsequent corresponding bandwidth demands.

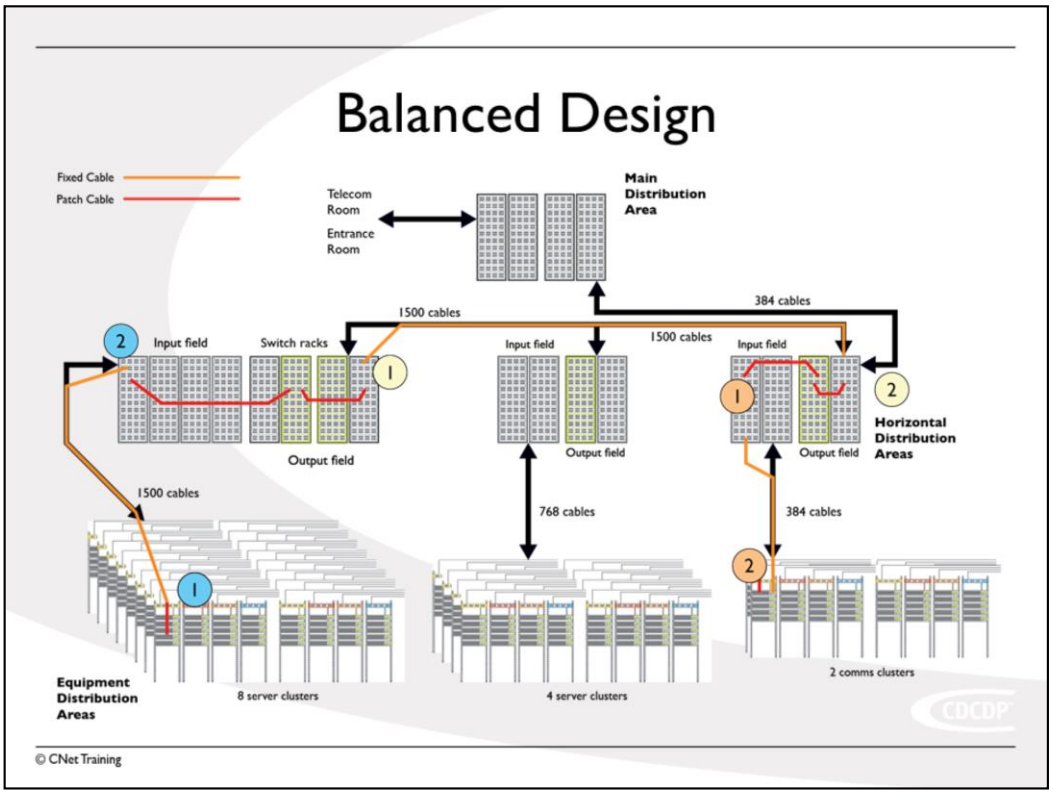


One option is to use a cable-intensive design. The key points are:

- Passive cabling, but lots of it
- Easy to hit the maximum number of connections allowed
- Need to remember maximum link length, and the length of inter-rack fixed cabling
- Low latency – effectively, it is a single physical channel

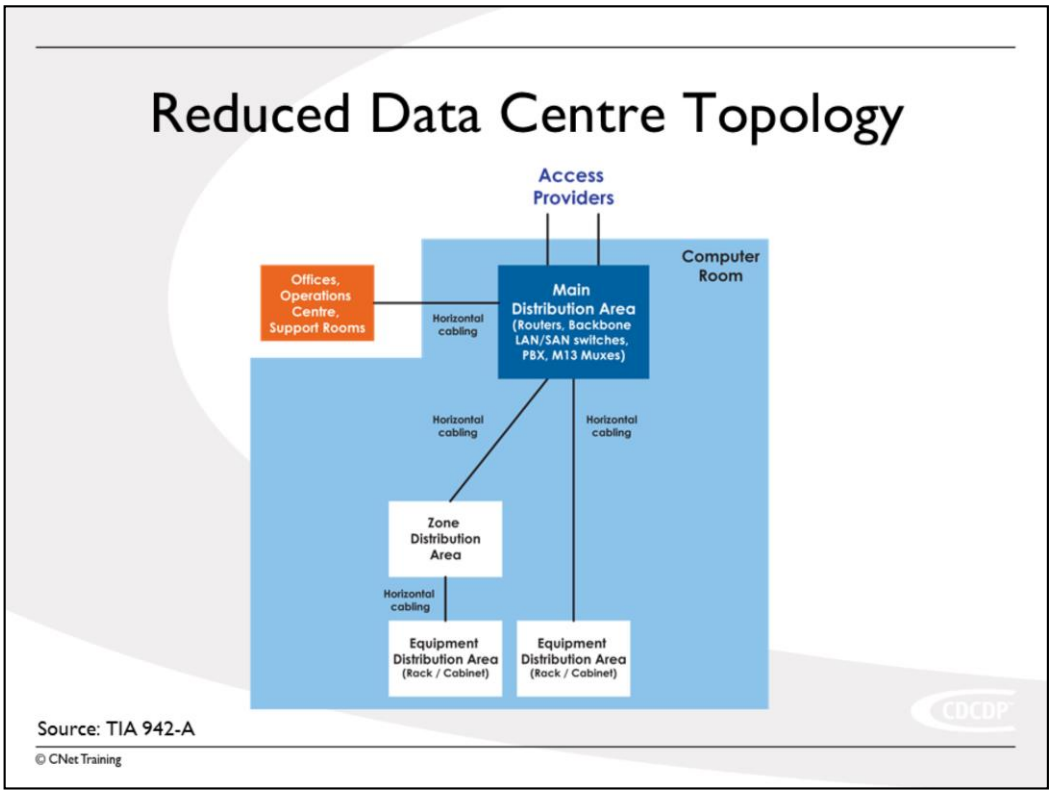


- This trend can be continued to the point where a 2-connector channel is implemented.
- This makes it easier to work within the 90m (295ft) fixed cabling distance limitations.
- Backbone cabling can be introduced into any or all of the inter-cluster connections; these can be fibre, allowing significant distance increase.
- The switches can provide resilience and diagnostic alarms.
- Many designers miss the point and install cable to the cable-intensive model, then overlay it with switches to the switch-intensive model.

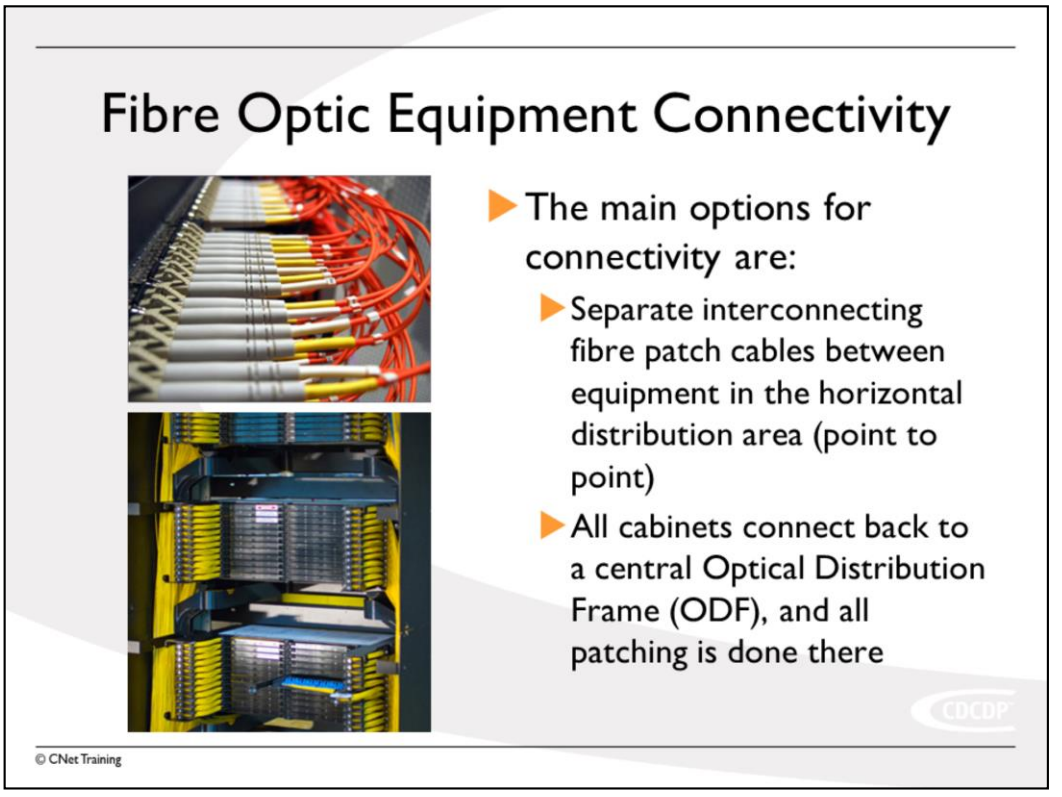


Active equipment can reduce the number of cables.

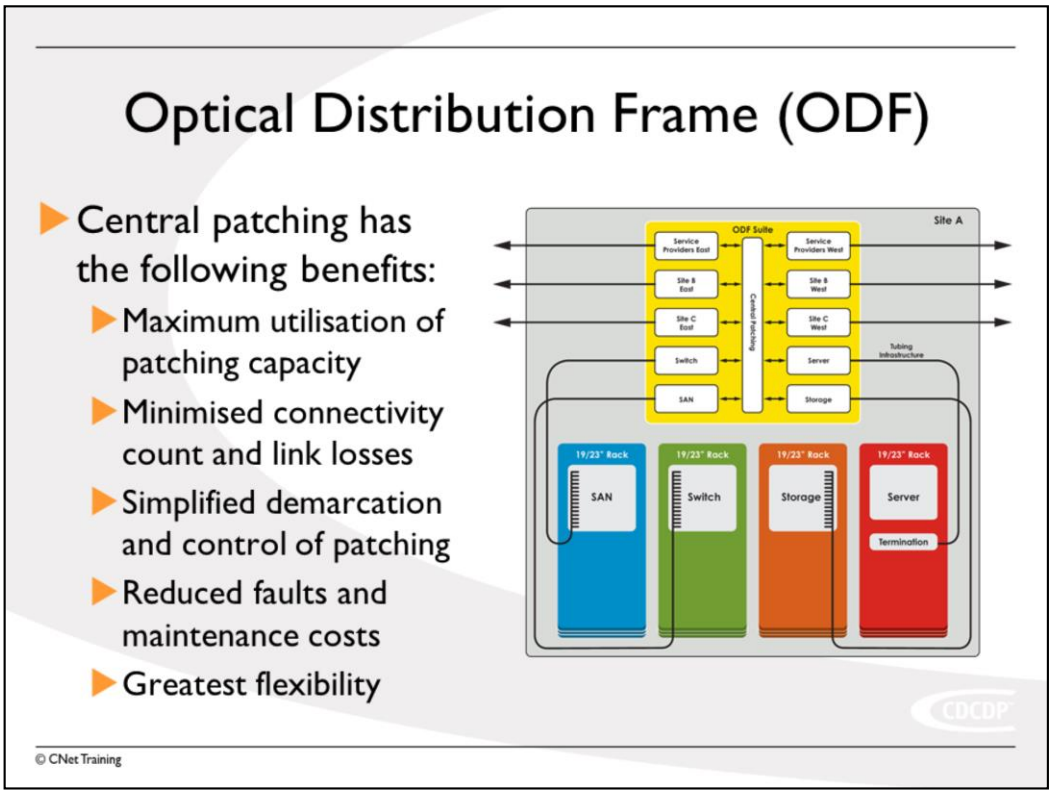
- Introducing switch racks into patching fields reduces the number of cables
- Introduces latency, requests are not serviced as quickly
- The cost is similar, save cable spend on switches



Data Centres can be complex or simplified. Data Centre designers can consolidate the main and horizontal cross-connects in a single MDA, possibly as small as a single cabinet or rack. The telecommunications room (for cabling support areas) and entrance room may also be consolidated into the MDA in a reduced Data Centre topology.



There are numerous options for connecting active equipment with fibre optic cables, but some have more merits than others for management and potential infrastructure growth.



It is important to identify the correct network configuration.

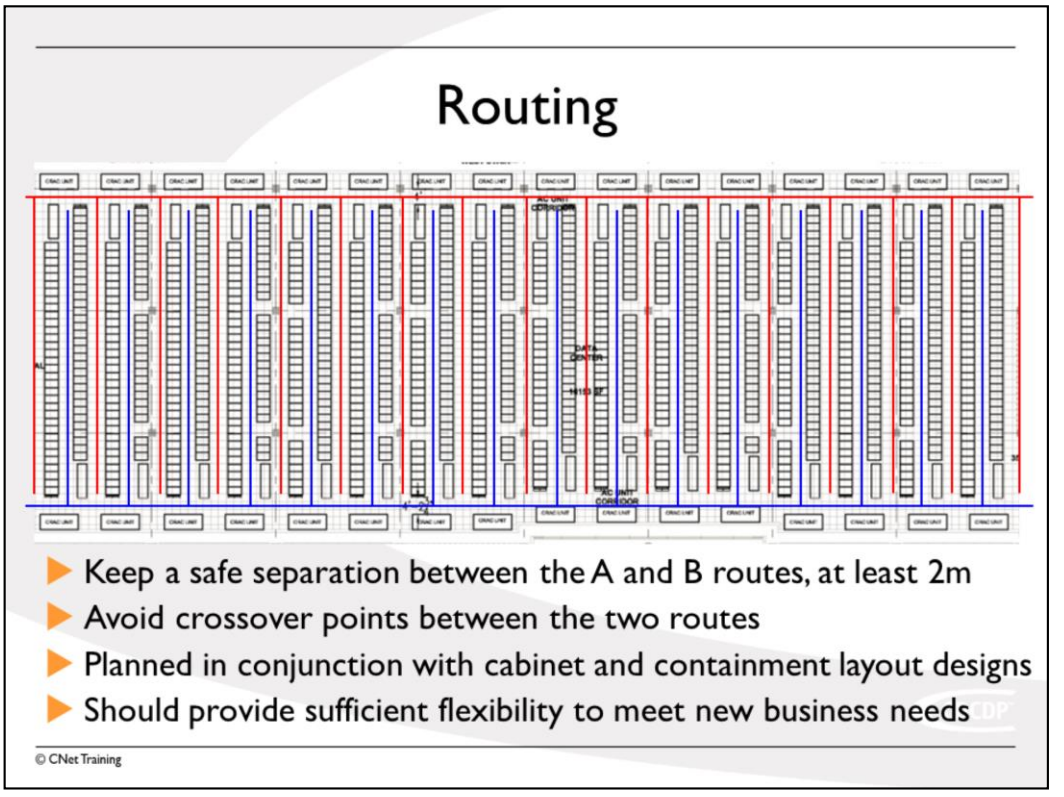
This configuration model illustrates a 'best practice' regime, providing complete transparency of connectivity via ODF patching between any two disciplines of equipment in a single network fabric.

The model shows the connectivity interfaces of SAN, switch, storage and server equipment extended through fibre to a single ODF with a central patching area.

It is essential to the efficient operability and maintainability of any distribution network that all equipment connections are extended from network element interfaces to a single termination and patching area (or two termination and patching areas where complete diversity / dual fabric is imposed).

The termination and patching area can constitute a single ODF or multiple ODFs: This regime demands a modular and expandable ODF design so any installation of multiple frames (to meet capacity requirements) will provide complete transparency of patching connectivity between frames. For example, multiple co-located frames can be configured and utilised as a single patching area.

If the central patching area is split between physical locations within a single fabric, the transparency of connectivity is lost and becomes fragmented. Complete connectivity can then only be established within the fabric by providing 'tie cabling' between patching areas within the fabric, which duplicates connectivity, increases link losses and reduces overall capacity. Suitable planning methods should be adopted to eliminate this scenario.



A good design should avoid single points of failure. This starts with correct routing of cables - here are two 'rules' to consider:

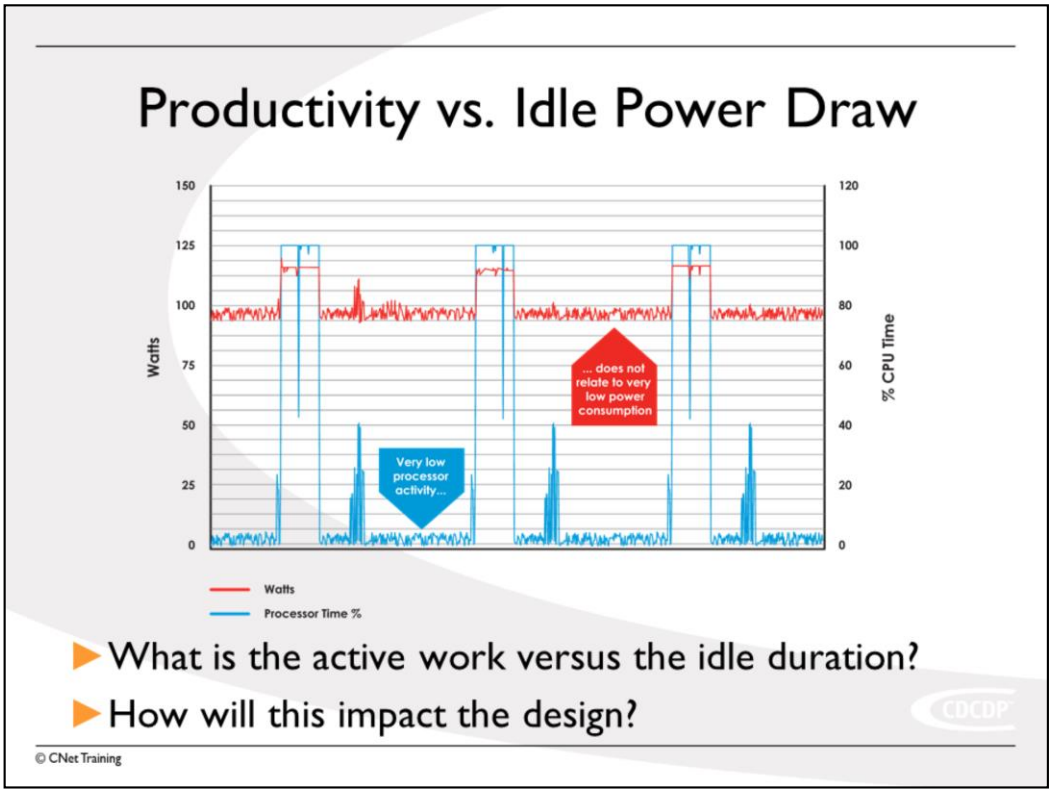
- Keep a safe distance between the A and B routes, at least 2m (6ft 7inch)
- Avoid crossover points between the two routes.

Remember This?

- Connectivity must maintain a tight bond between IT and the infrastructure
- Must accommodate many and varied applications
- Must be flexible to upgrade - supporting new technologies and equipment installations whilst meeting operational SLAs
- The CDCD must be aware that a change in IT hardware may have a direct impact upon the design
- Periodic design reviews are a recommended practice

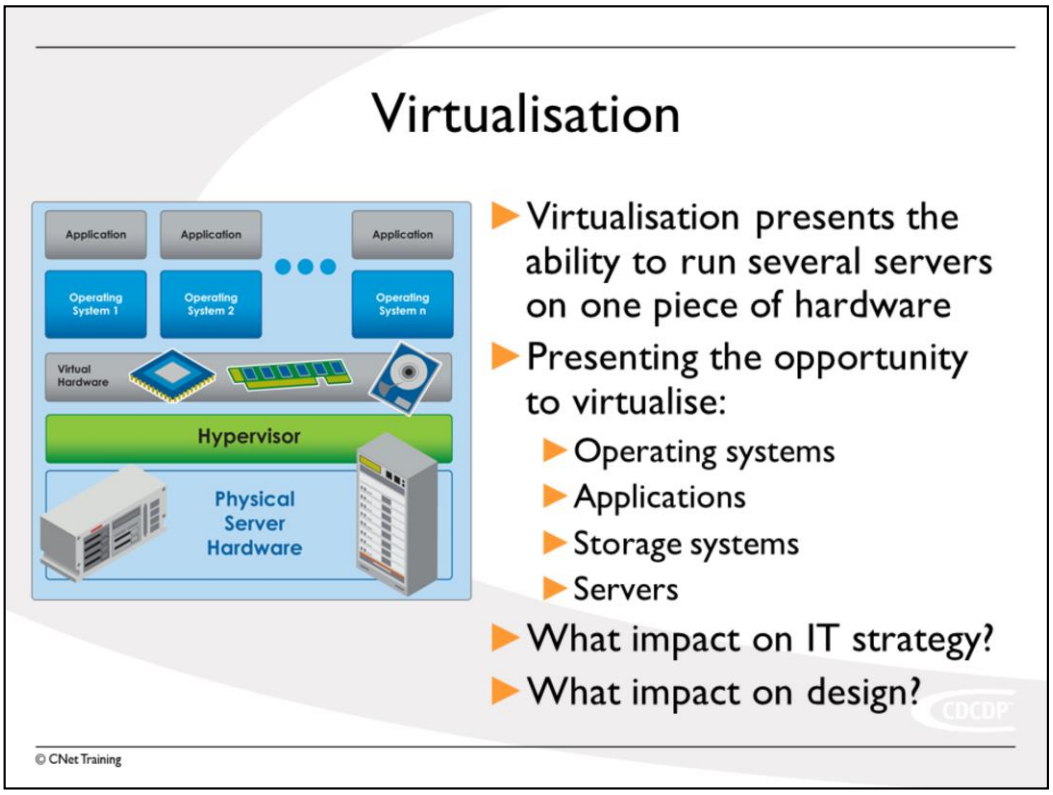
CDCDP

© CNet Training



Processors continue to consume power even when they are idle.

Virtualisation is now a recognised practice to reverse this lack of productivity; it ensures more activity is carried out by running processors harder at all times, increasing the power required by the processor, but reducing the number of CPUs required.

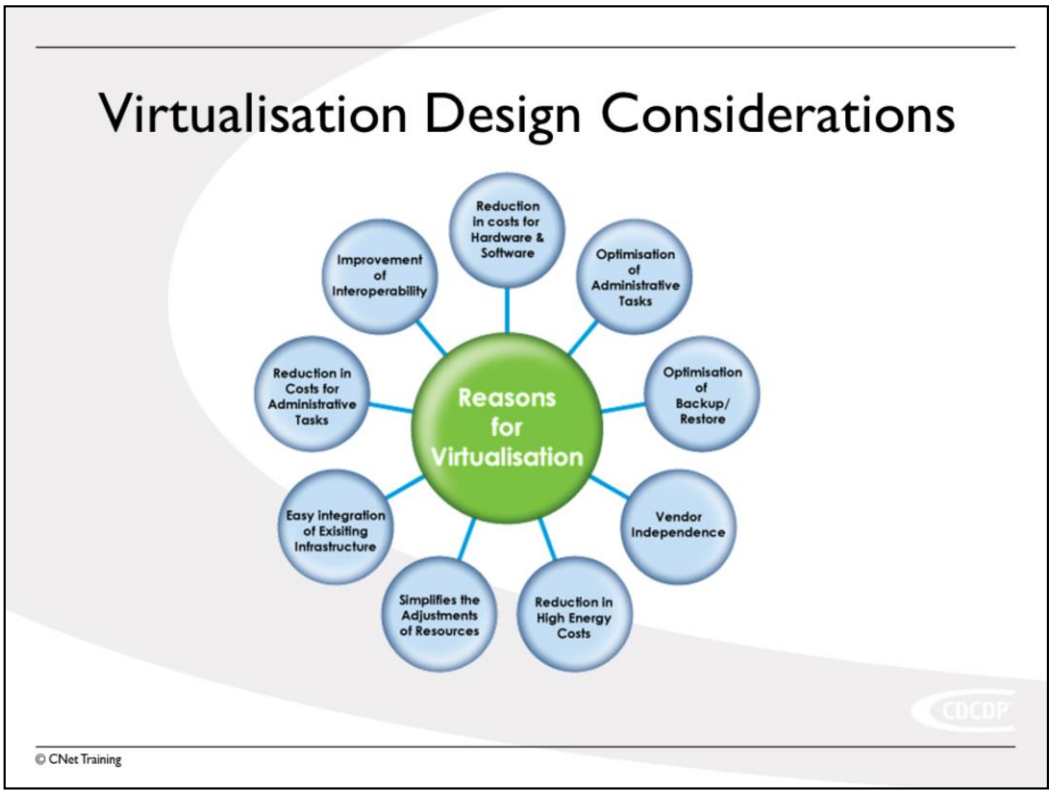


Virtualisation is the ability to replace a number of physical servers with virtual servers, running on a single physical server.

Virtual servers can run directly on top of the hardware, or via a Hypervisor layer which links them to the physical world.

Different operating systems can be run in parallel, as well as instances of applications, e.g., Oracle. There may be issues with licensing and support which need to be investigated in detail.

The impacts of virtualisation on IT Strategy can be profound, and the CDCD must understand and allow for them in the design.



Virtualisation has introduced potential cost saving benefits to businesses, providing a rapid ROI through lower management cost and enhanced asset utilisation. Apart from the main cost incentives, virtualisation can introduce numerous benefits, such as:

- Expanded flexibility
- Reduction in software and hardware assets
- Rapid application deployment
- Improvement in interoperability and functionality

As with any Data Centre transformation initiative, a business must consider the advantages against the projected impact upon the business (short and long-term). Before stepping into the world of virtualisation, there are three key steps that should be addressed to ensure a successful implementation:

1. Define your Data Centre strategy to align with business requirements.
2. Perform in-depth and honest assessments of the current Data Centre.
3. Determine the most important projects that will benefit from virtualisation.

The CDCD will need to work closely with the IT Architect to fully understand infrastructure requirements for planned and projected virtualisation environments.

Observations?

- Virtualisation changes connectivity requirements - Needs more (or less)?
- Speeds are increasing - Computer and networking
- Connectivity distances are decreasing
- Cabinet densities are increasing
- Heat generation is concentrating
- Others?

© CNet Training

There are some common threads that can be observed in these developing technologies.

Design Strategies

- Design must be flexible to upgrade - support new technologies and equipment installations whilst meeting operational requirements
- Smaller connectivity zones
- Higher-speed uplinks
- Zone different activities
- Modular build when required

© CNet Training

There are a number of approaches that have developed to increase the flexibility of the design.

Review

- Can you?
  - Understand the tight link between IT strategy and the Data Centre
  - Identify network topology options
  - Explain connectivity options
  - Discuss the IT subsystems

© CNet Training

Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®) Core Unit

Copper and Optical Fibre Cable Connectivity

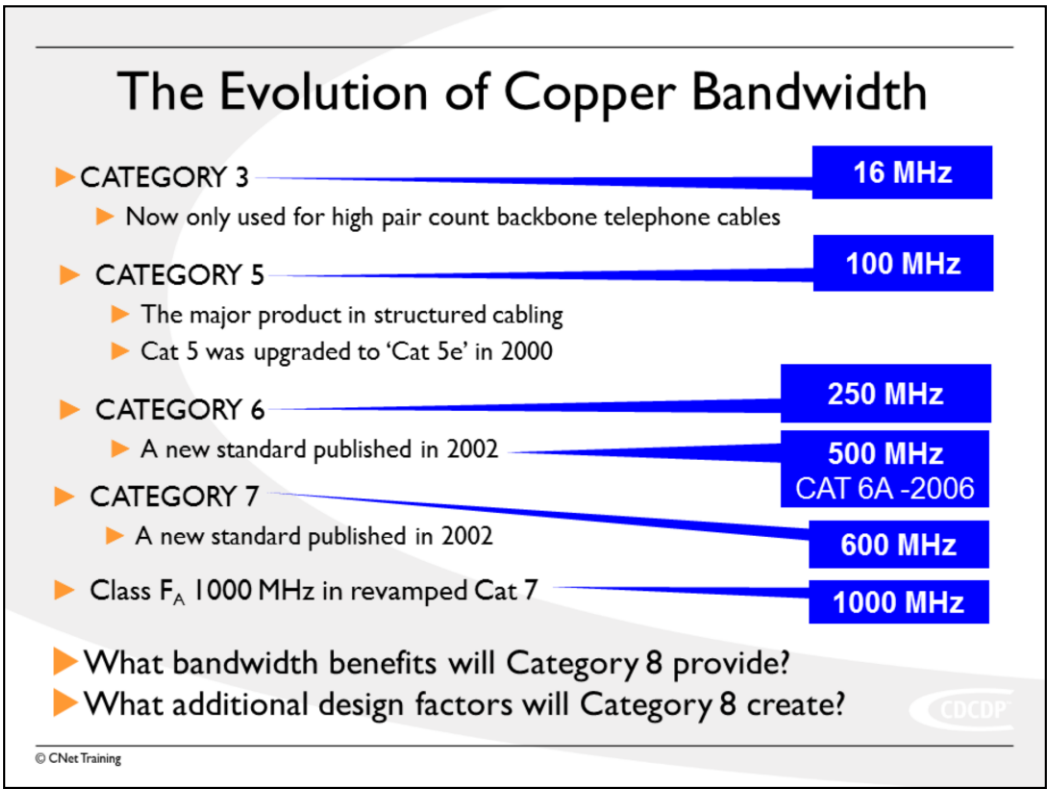
Version 1509

CDCDP

Objectives

- At the end of this module you will be able to:
  - Identify some of the copper and optical fibre component options
  - Identify some of the copper and optical fibre design options
  - Identify their operational suitability
  - Discuss which option to choose

© CNet Training



The cabling Standards define performance characteristics according to the information carrying capacity or bandwidth of a cable type. In the US, performance is indicated by category - for example, Cat 5e. ISO/IEC and CENELEC Standards classify the performance of a channel - for example, Class D.

They all have the same or similar meaning: How many bits per second are they capable of transferring from one point to another. This question is especially critical with the increasing bandwidth demands now being transmitted across copper channel links.

TIA-942-A Recognised Cables

- 4-pair 100 Ohm balanced twisted-pair cable (ANSI/TIA-568-C.2), Category 6 or Category 6A, with Category 6A recommended
- 850nm laser-optimised 50/125um multimode fibre cable - OM3 or OM4 (ANSI/TIA-568-C.3), with OM4 recommended
- Singlemode optical fibre (ANSI/TIA-568-C.3)
- 75ohm (734 and 735 type) coaxial cable (Telcordia Technologies GR-139-CORE)
  - Used for T1, T3, E1, and E3 circuits only

© CNet Training

TIA-942-A makes recommendations on cable types. For Data Centres in the US, these Standards will apply. How does this compare to European Standards?

EN 50173-5 Cable Requirements

- Balanced cables:
  - The electrical performance of balanced cables shall meet the Category 5, 6, or 7 requirements of EN 50173-1
  - Multimode optical fibre cables:
    - The cabled optical fibres shall meet the Category OM3 and OM4 (50/125um) requirements of EN 50173-1
  - Singlemode optical fibre cables:
    - The cabled optical fibres shall meet Category OS1 or OS2 requirements of EN 50173-1

© CNet Training

For Data Centres in Europe, different terminology is used and it is important for the CDCD to understand similarities and differences.

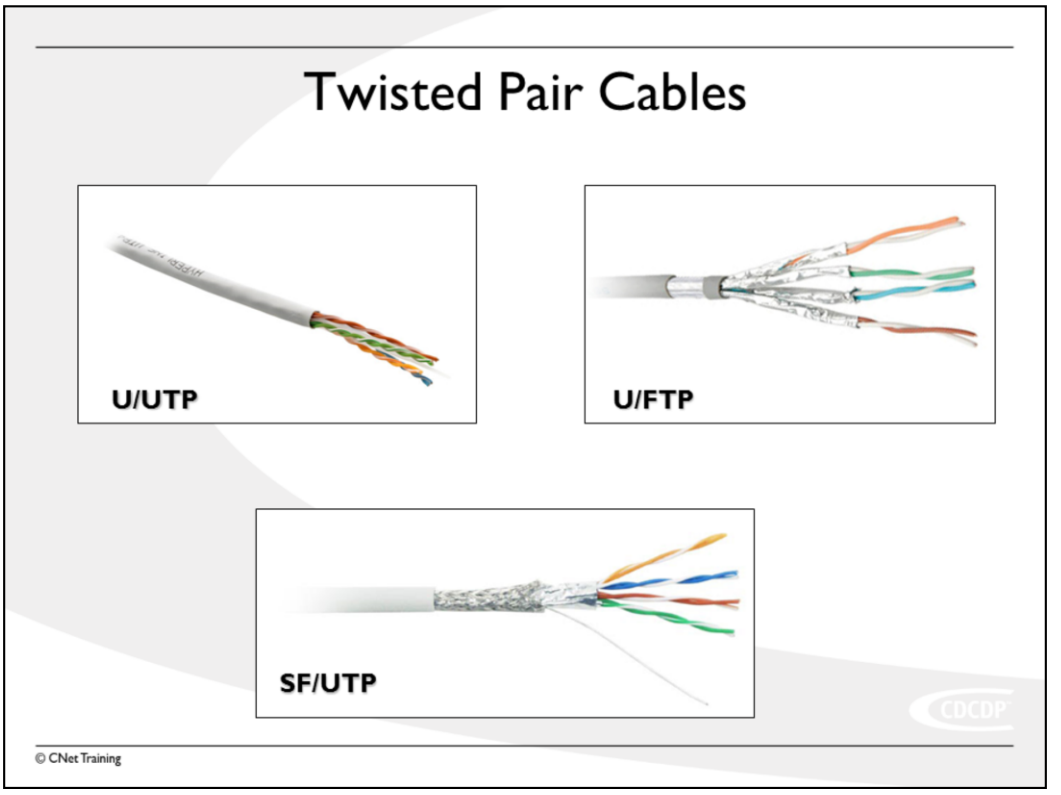
ISO 11801 - Cable Definitions

- U/UTP: Completely unscreened
- F/UTP: One foil screen around the whole cable
- U/FTP: A foil screen around each pair
- SF/UTP: A foil and a copper braid around the whole cable
- S/FTP: A foil around each pair, and a copper braid around the whole cable

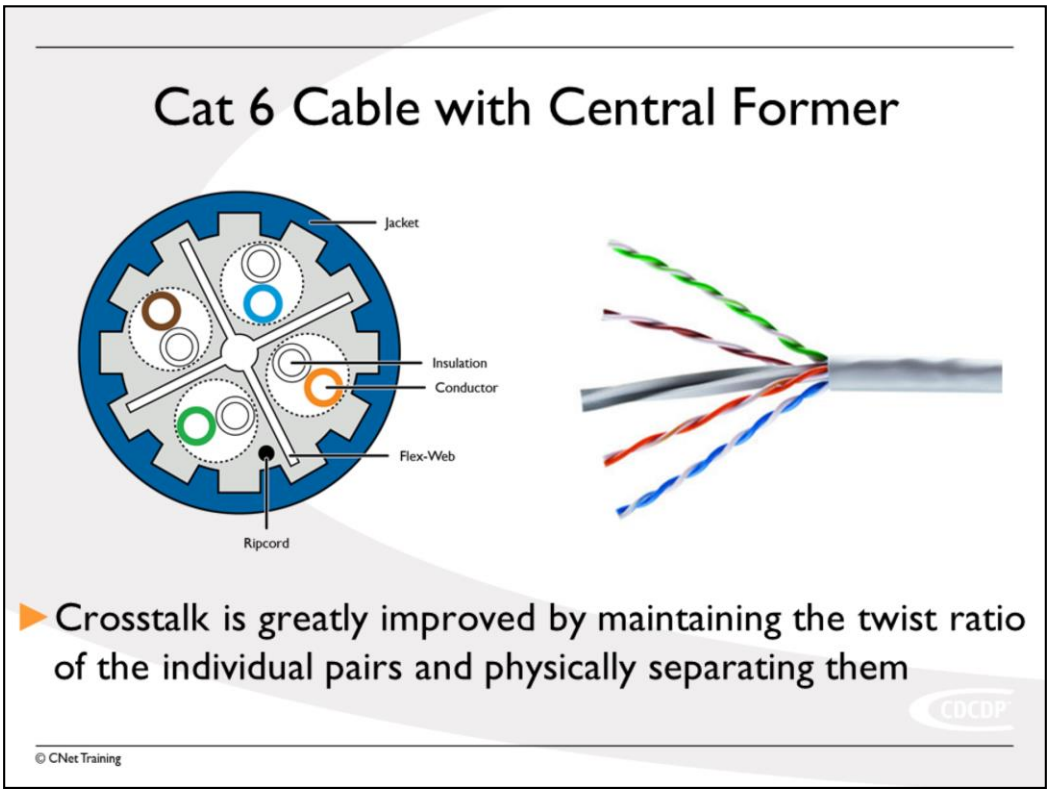
Note: The letters before the '/' denote what goes around the whole cable; what follows the '/' denotes what goes around each pair

© CNet Training

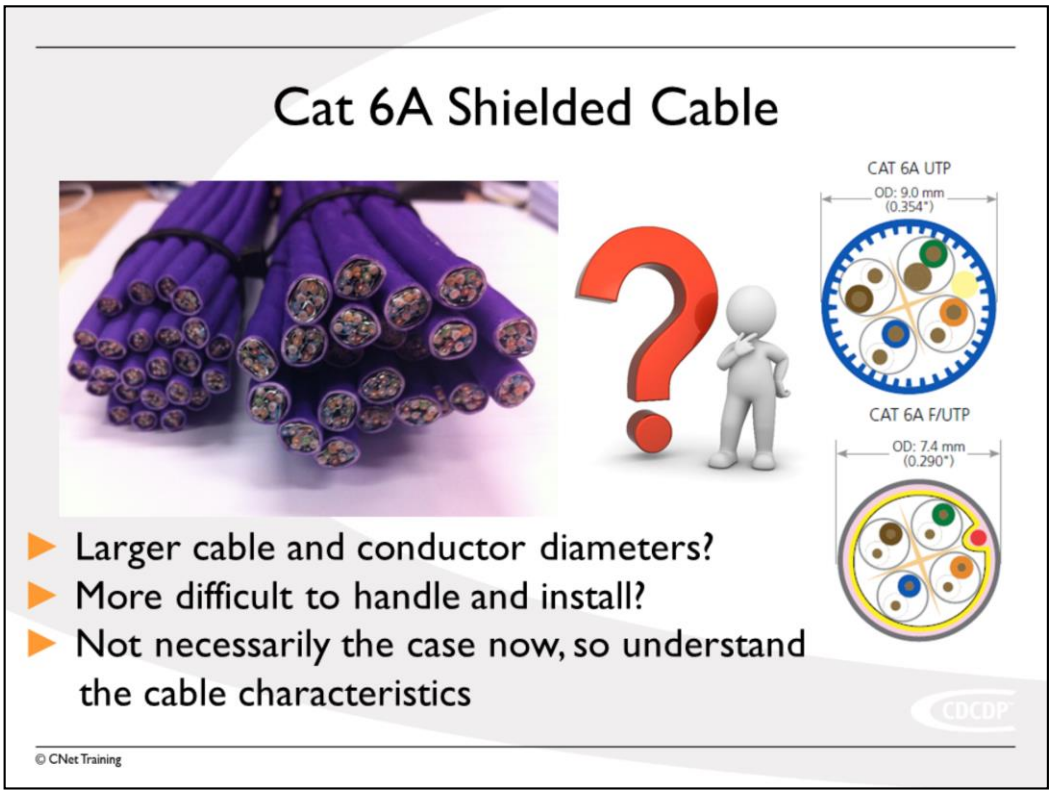
Screening or shielding improves performance by mitigating the effects of both internal and external interference. Crosstalk is the main concern for installed twisted-pair cabling, mostly from within the cable sheath itself. With today's high frequency applications, such as 10GBASE-T, external crosstalk (otherwise known as alien crosstalk) can be a problem, particularly in unscreened cabling.



Screened cables are more complex.



There are many different ideas on how best to separate the pairs, but they can result in a larger cross-sectional area (CSA). As a result, a cable bundle is significantly bigger. This is something that presents a challenge to the CDCD, and he / she needs to take account of the resultant space and containment requirements throughout the Data Centre.



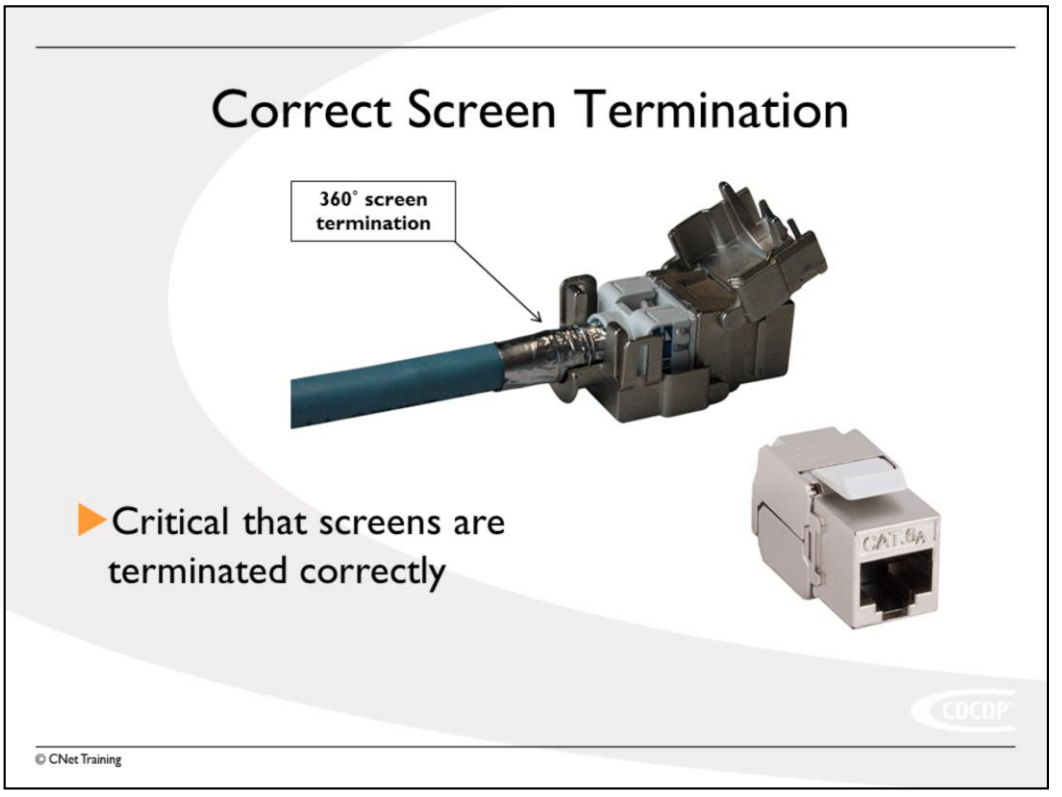
Larger cable and conductor diameters, and the increased stiffness of augmented Category 6 and FTP cables, have a significant impact on standard installation practices. Is this actually the case? Although shielded cable has always had the reputation of being bigger, bulkier, and more difficult to handle and install, this is now not necessarily the case. Some Cat 6A F/UTP cable specifications can be smaller than the standard Cat 6 UTP applications.

Another factor that needs to be considered: The cable bend radius will vary, depending on the cable condition during installation (tensile load) and after installation, when the cable is at rest (no load). The minimum inside bend radius (under no-load conditions) for installed, four-pair UTP cable shall be four times the cable diameter, per ANSI/TIA/EIA-568-B.

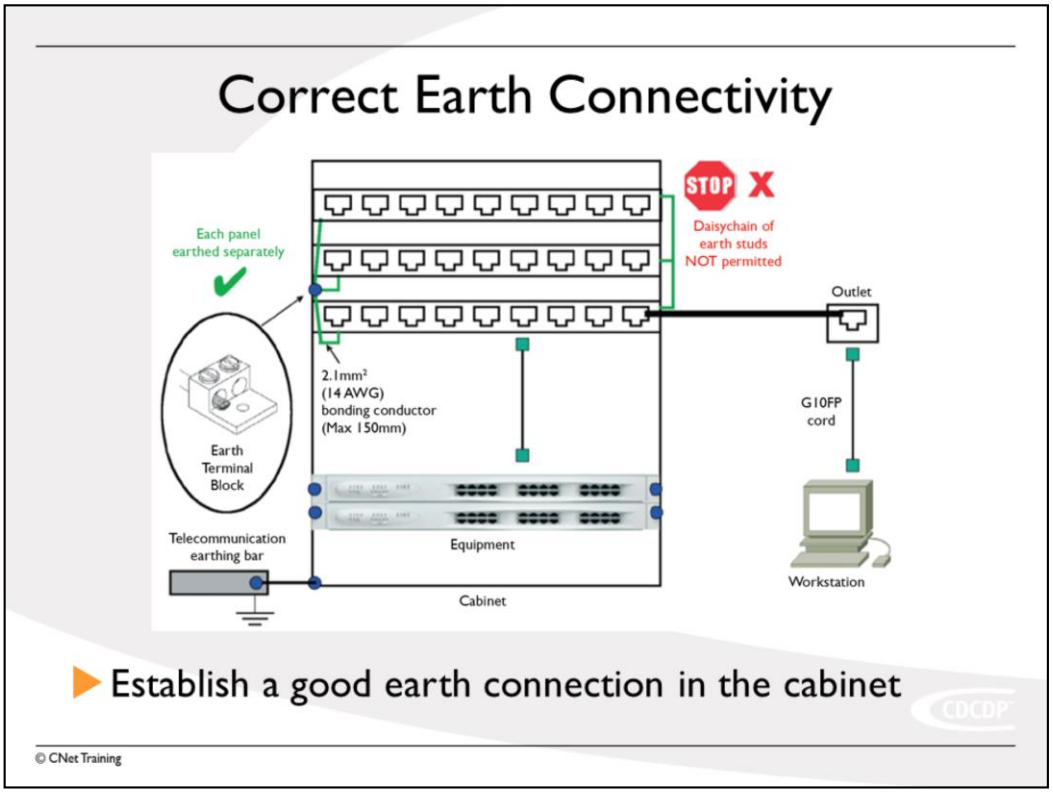
Category 7A / Class F_A

- Category 7A
  - Fully shielded cable
  - Individual foils around each pair coupled
  - High-screen coverage outer braid, providing immunity from outside interferences
  - Optimises channel performance
  - Operates at frequencies up to 1000 MHz
- Is Category 7A replacing Category 6 / 6A within today's Data Centre designs?

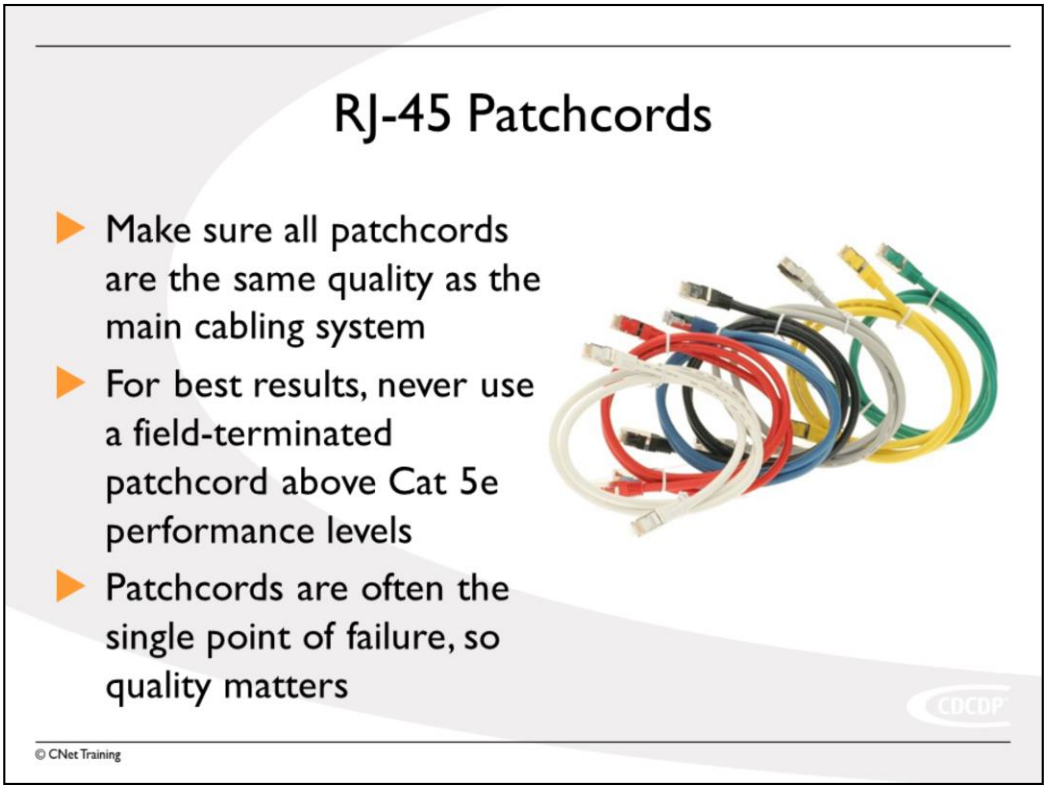
© CNet Training



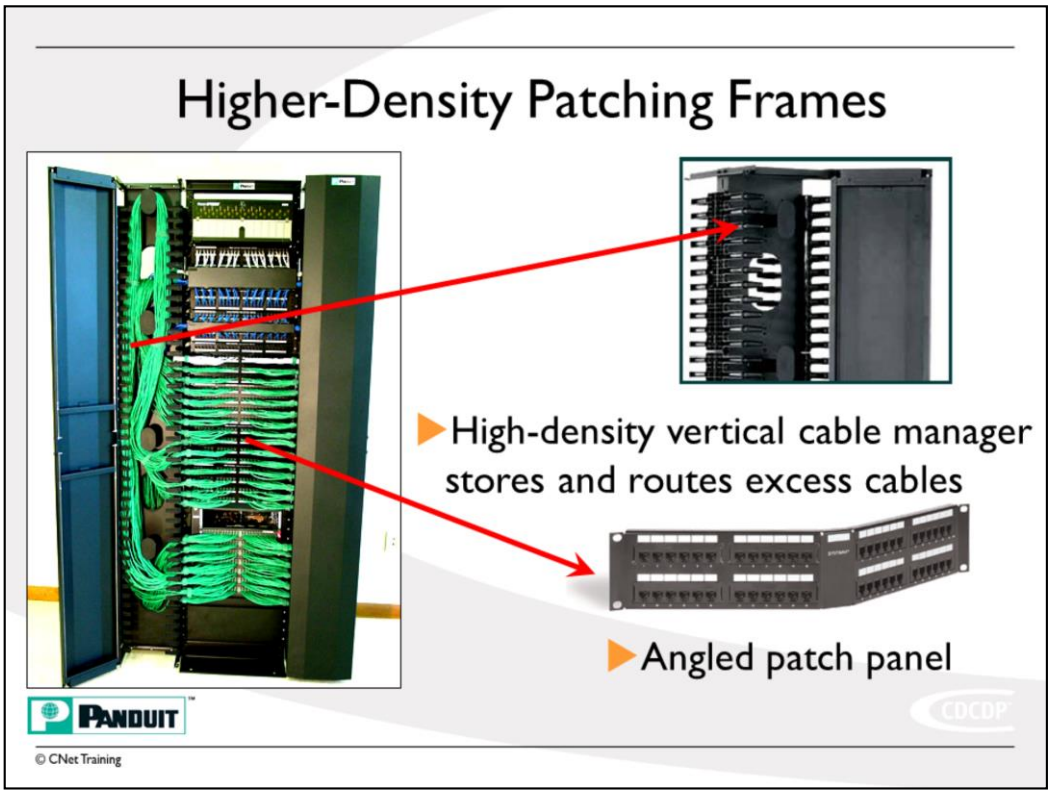
With screened cables, it is critical that screens are terminated correctly. This requires the installer to be properly trained in the appropriate techniques.



It is equally vital the metalwork in the rack is properly earthed, and does not rely solely on the mounting screws.



Patchcords are the cause of 80% of problems in data networks. They are part of the cable system and should be treated with the same respect as the rest of the installation. For best results, never use a field-terminated patchcord above Cat 5e performance levels.



Manufacturers have introduced new, innovative patching solutions. Angled patch panels are not suited to cabinet installation, due to the need to block off the triangle of space at the top and bottom of the panel that allows air through. Be careful of blocking the door if used in a cabinet.

High-Density Patching Frames

- Patch panels or 110 punch-down applications supporting Category 6
- Main distribution areas (MDAs) to server and switch environments

BELDEN
SENDING ALL THE RIGHT SIGNALS

CDCDP

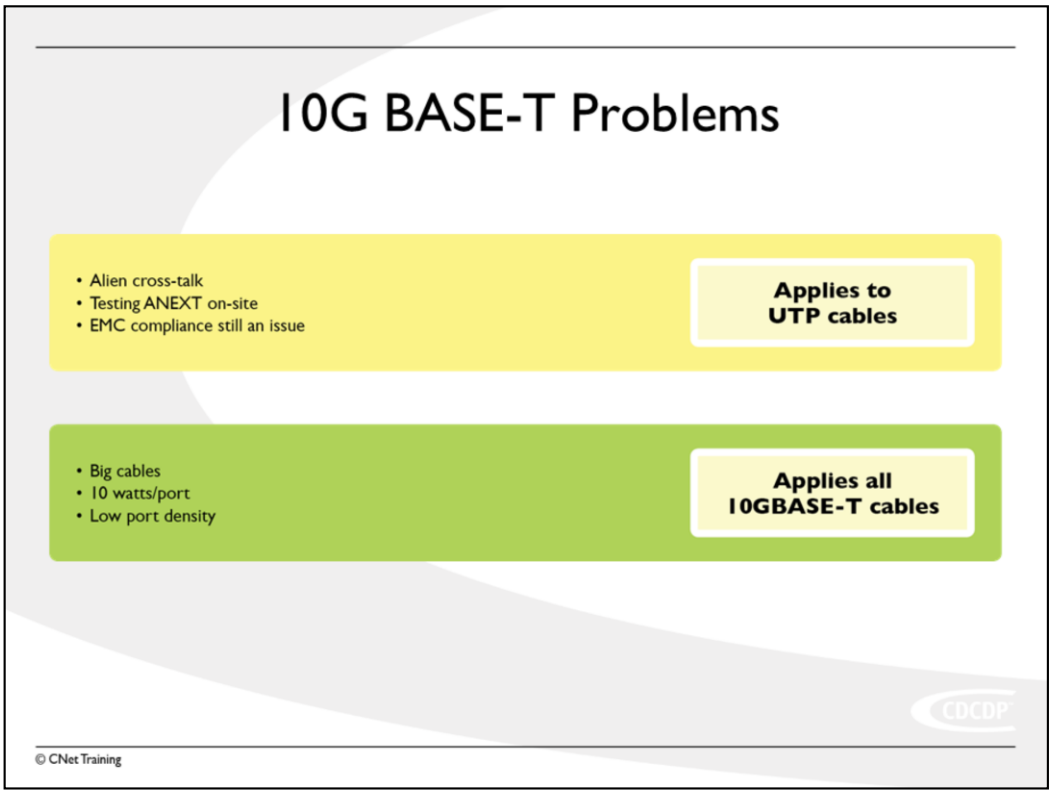
© CNet Training

Copper Cable Design Issues

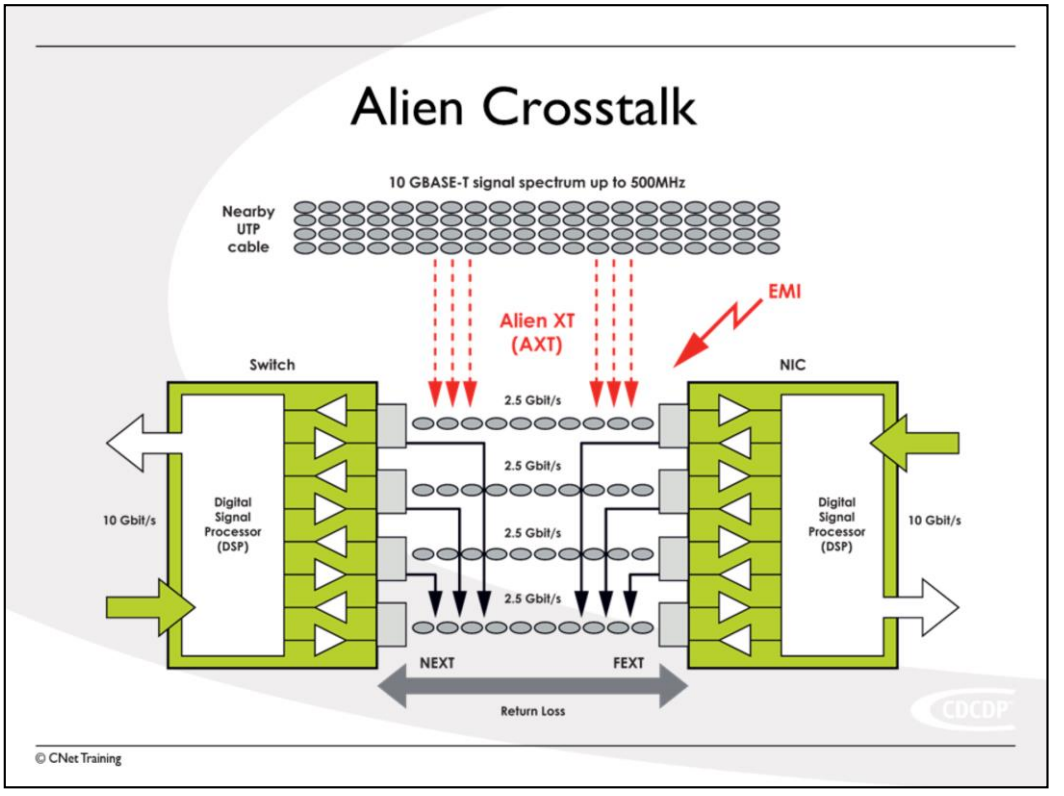
- Copper cabling gives additional problems for the CDCD to mitigate
  - Cable size increases containment
  - Increased bend radius increases containment
  - Increased size reduces packing density
  - Increased containment weight
  - Alien crosstalk becomes an issue

© CNet Training

There are issues that appear on 10G Ethernet and above with copper cabling. The CDCD must mitigate these.



10Gbps over copper has a number of technical hurdles to overcome.



A range of new measurements are required to test copper cables at 10Gbps data rates:

- Power Sum Attenuation to Alien Crosstalk Ratio at the Far End (PSAACRF)
- Alien Equal Level Far End Crosstalk (AELFEXT), Alien Far End Crosstalk (AFEXT), Alien Near End Crosstalk (ANEXT), Power Sum Alien Far End Crosstalk (PSAFEXT), Power Sum Alien Near End Crosstalk (PSANEXT)
- Plus the usual suspects of Attenuation / Insertion Loss, Return Loss, Near End Crosstalk (NEXT), Far End Crosstalk (FEXT), Attenuation Crosstalk Ratio (ACR), etc.

Solving Alien Crosstalk

- There are two basic ways to solve alien crosstalk:
  - Physical distance between interfering item and victim
  - Earthed metal screen between them

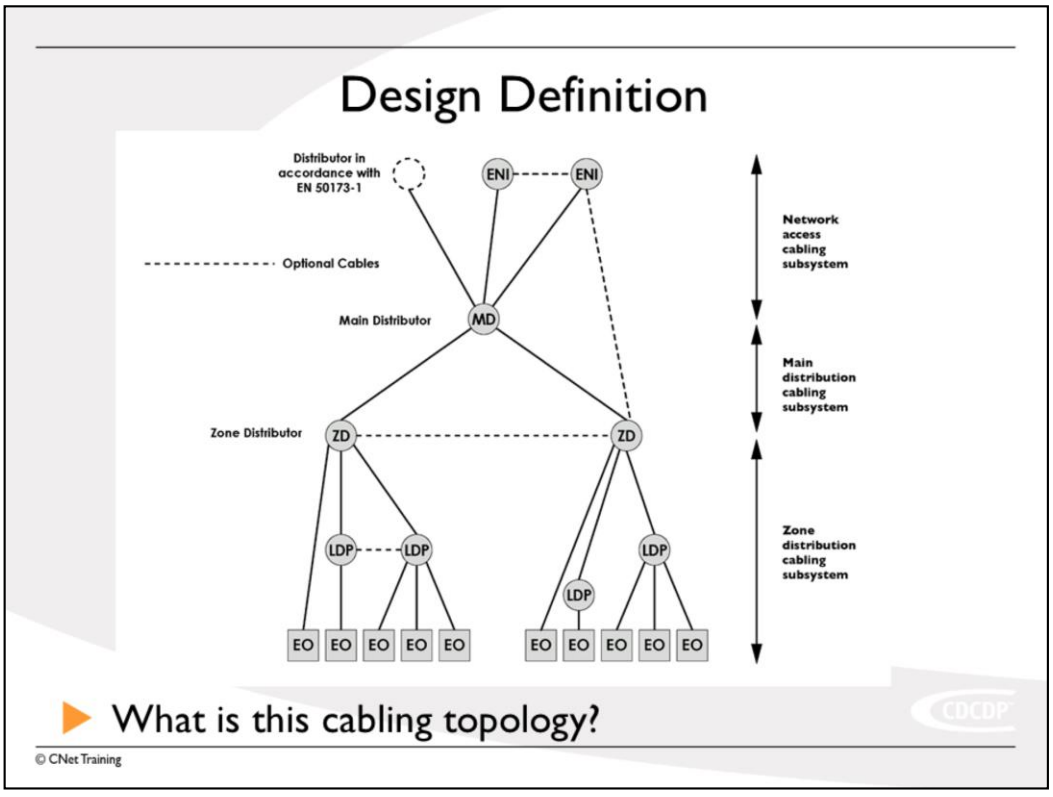
© CNet Training

As ever, there are some simple parameters that physics dictates.

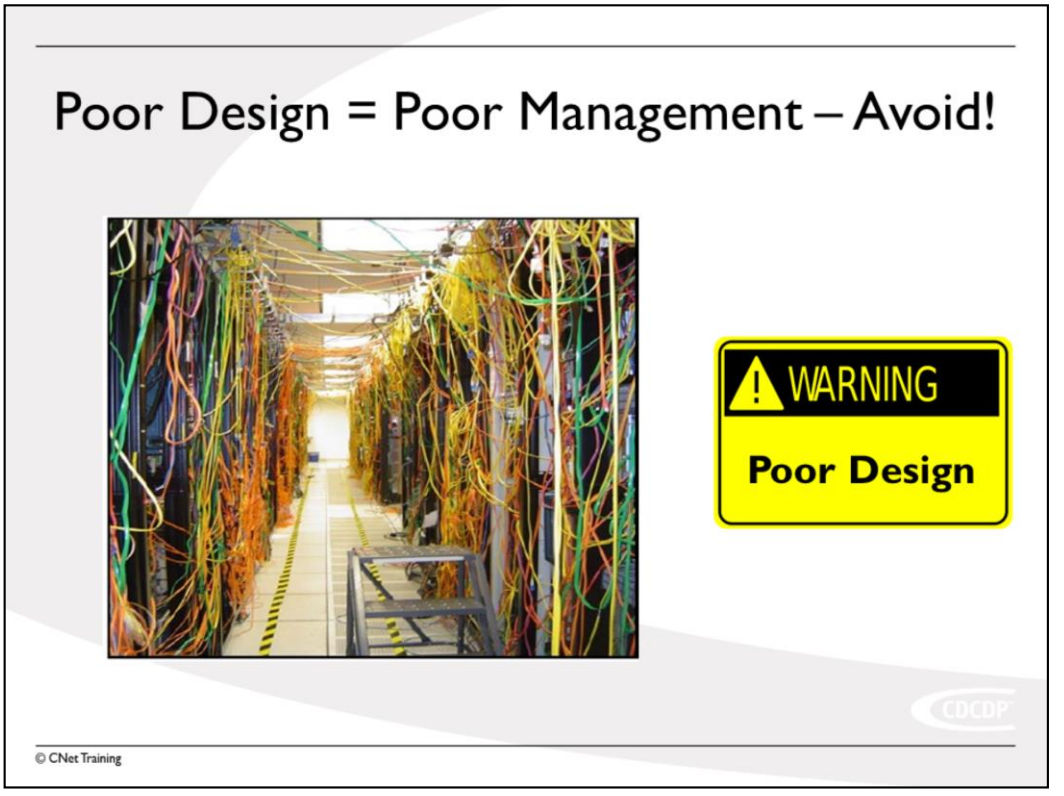
Any Questions?

- Are there any questions before we move onto some system design issues?

© CNet Training



Any design should be in line with the definitions of the Standard. However, be aware of the differing technical language between various Data Centre Standards.



Unfortunately, cabling can become quite untidy when it is not managed correctly:

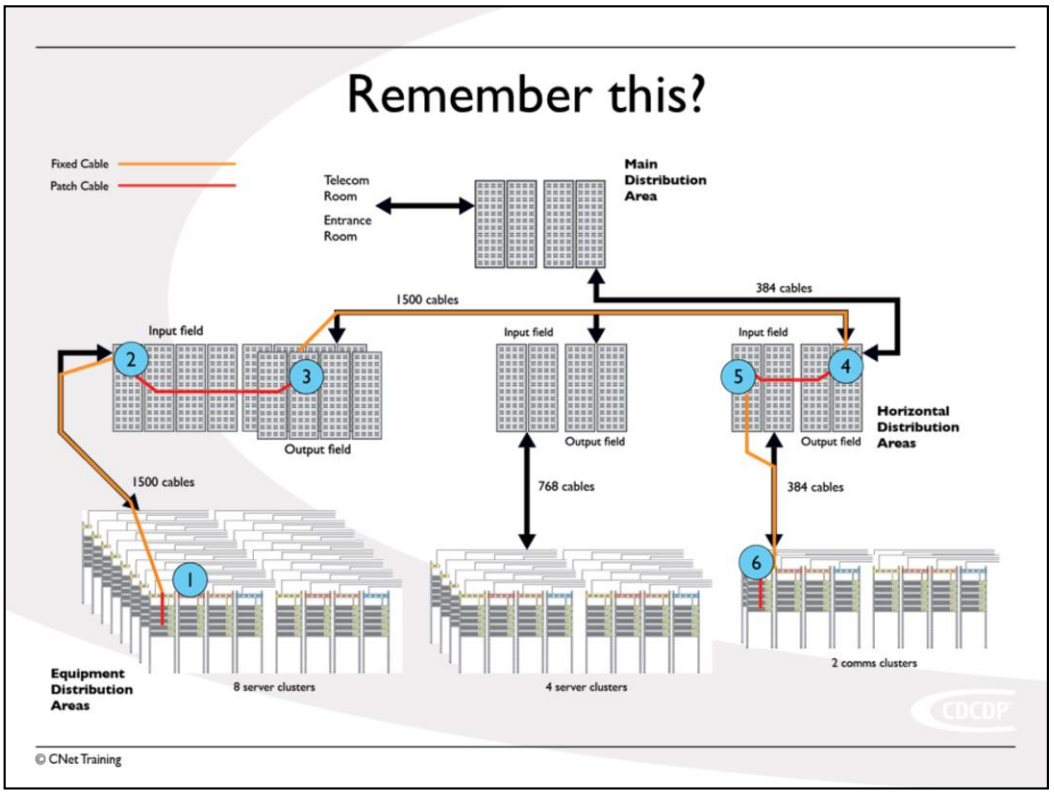
- No defined cable paths
- Poor discipline at the active equipment
- Fault identification issues
- Poor decommission policies
- Poor underfloor discipline control

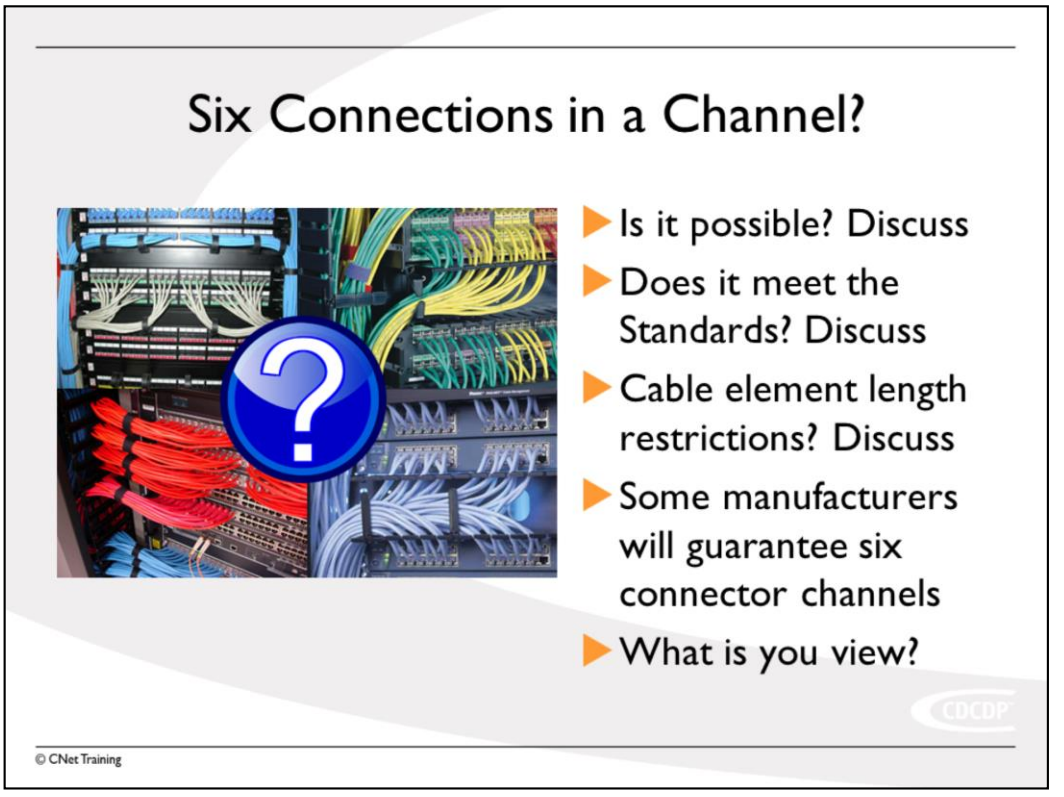
Best Generic Design?

- Not a huge price difference between cable-intensive or switch-intensive design
- Take a realistic view on resilient/redundant paths and components
  - Cable-intensive gives:
    - Less latency
    - Less heat generated
    - Others?
  - Switch-intensive gives:
    - Many more points of failure
    - More heat generated
    - More latency, due to numerous switch paths
    - Better manageability
    - Others?
- Put in enough cable to give IT personnel the option!

© CNet Training

The choice may not be simple, but the CDCD must allow for the needs of the organisation and appreciate future growth expectations.


Remember this?
Fixed Cable
Patch Cable
Telecom Room
Entrance Room
Main Distribution Area
1500 cables
384 cables
Input field
Output field
Input field
Output field
Input field
Output field
Horizontal Distribution Areas
1500 cables
768 cables
384 cables
Equipment Distribution Areas
8 server clusters
4 server clusters
2 comms clusters
© CNet Training

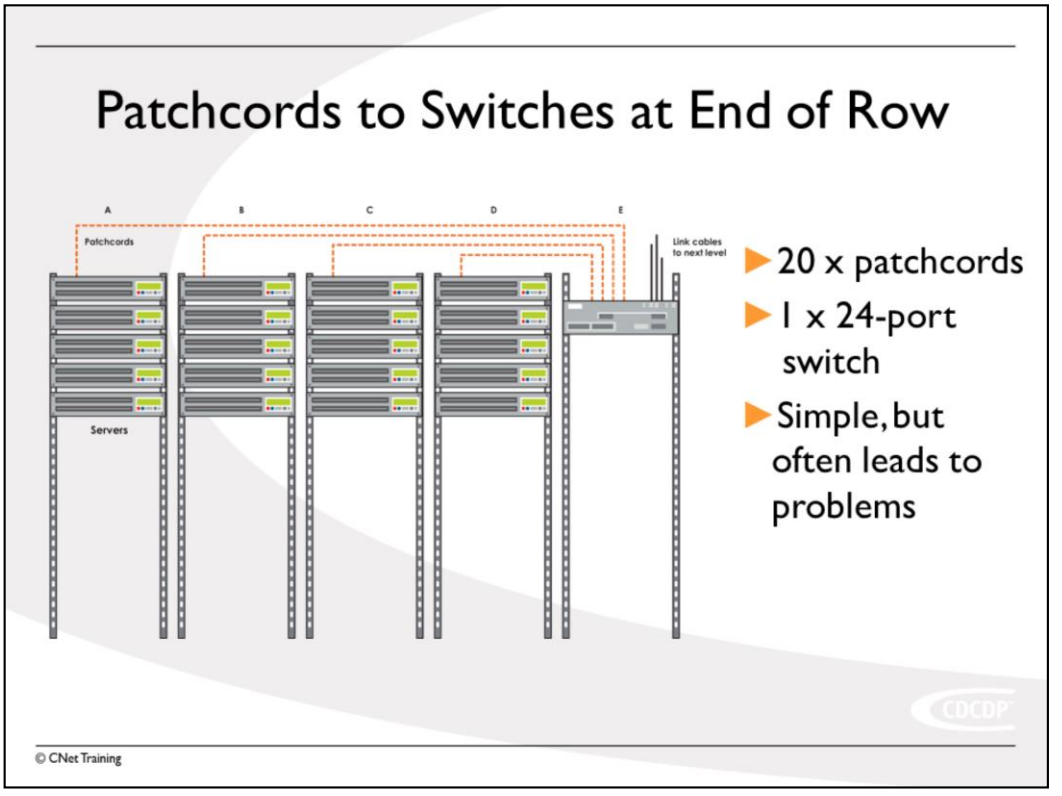


Most major manufacturers will now support a six connector channel design to enable cabling to be used in a Data Centre.

Design and Growth Management

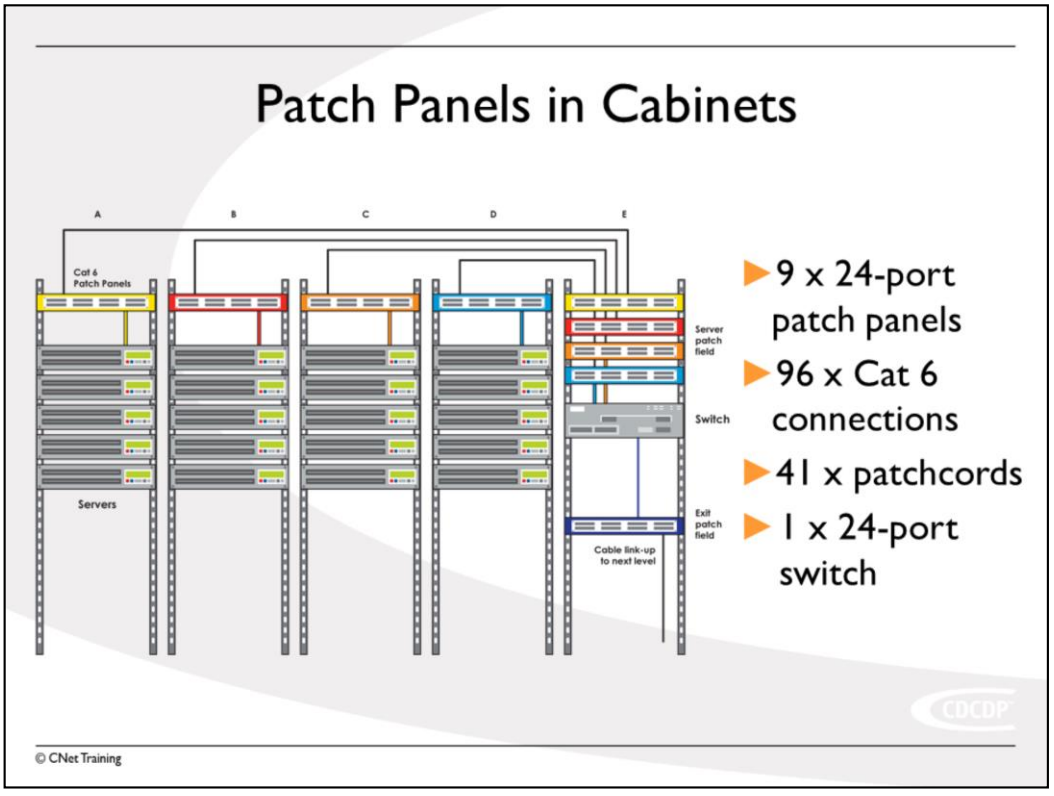
- Check the number of connections in the channel
- Four maximum (or more if guaranteed by a manufacturer)
- Obey channel length restrictions of maximum 100m (328ft)
- Understand bandwidth-to-distance impacts
- Use quality cabling of the same category and fibre type
- Test in accordance with relevant Standards
- Additional cable deployment needs to be fast and (ideally) in normal working hours
- Redundant cable should be easily recovered

© CNet Training



There are several different design options for interconnections between equipment. This one has patchcords from each piece of equipment to switches at the end of the row. The uplink to the next level is made from the end of row switch.

Patchcords can be difficult to manage, and it is easy to make a 'wall of patchcords' if the system is badly controlled.



This option has internal patchcords from the equipment to the patch panel at the top of the rack. The links to the end of the row are permanent cabling.

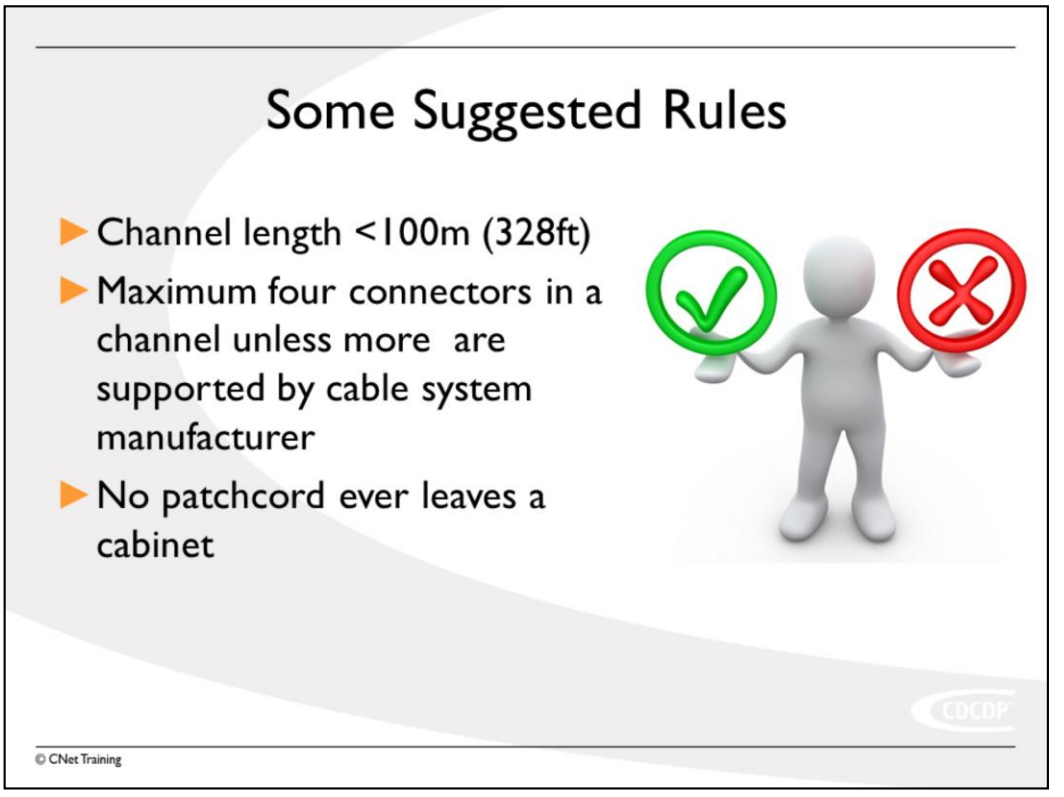
The number of patchcords can be affected by the topology of the design.

Example:

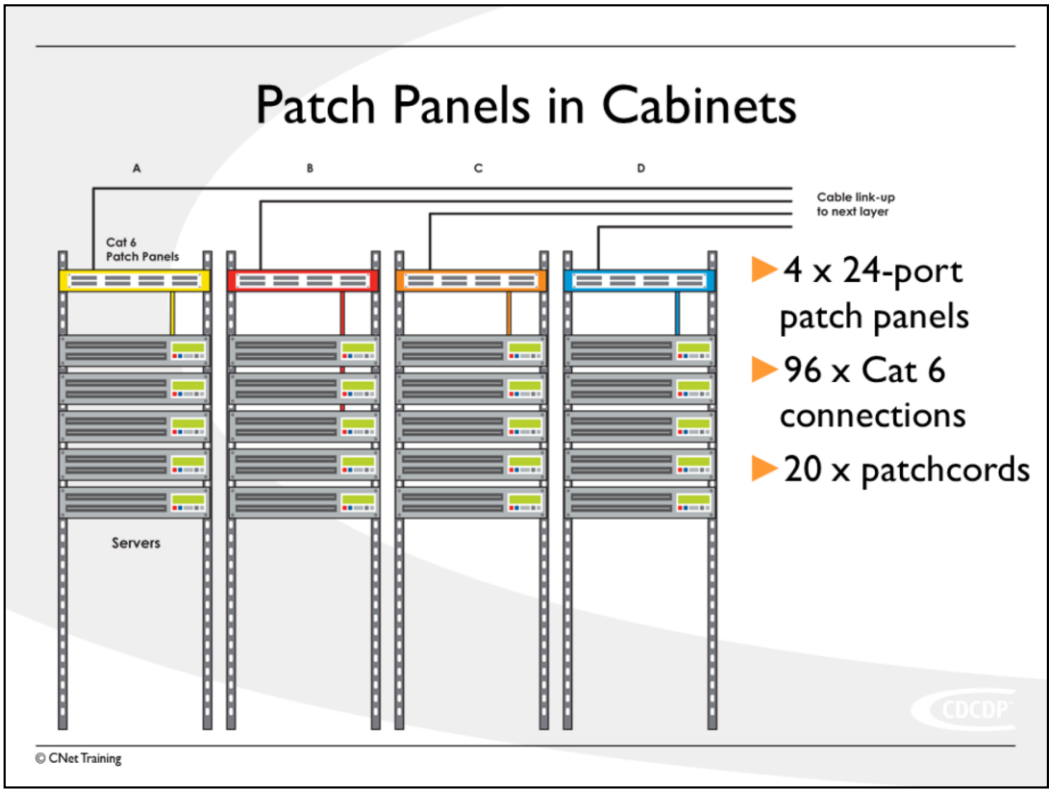
1 panel per rack

1 patch field per cluster

1 switch per cluster

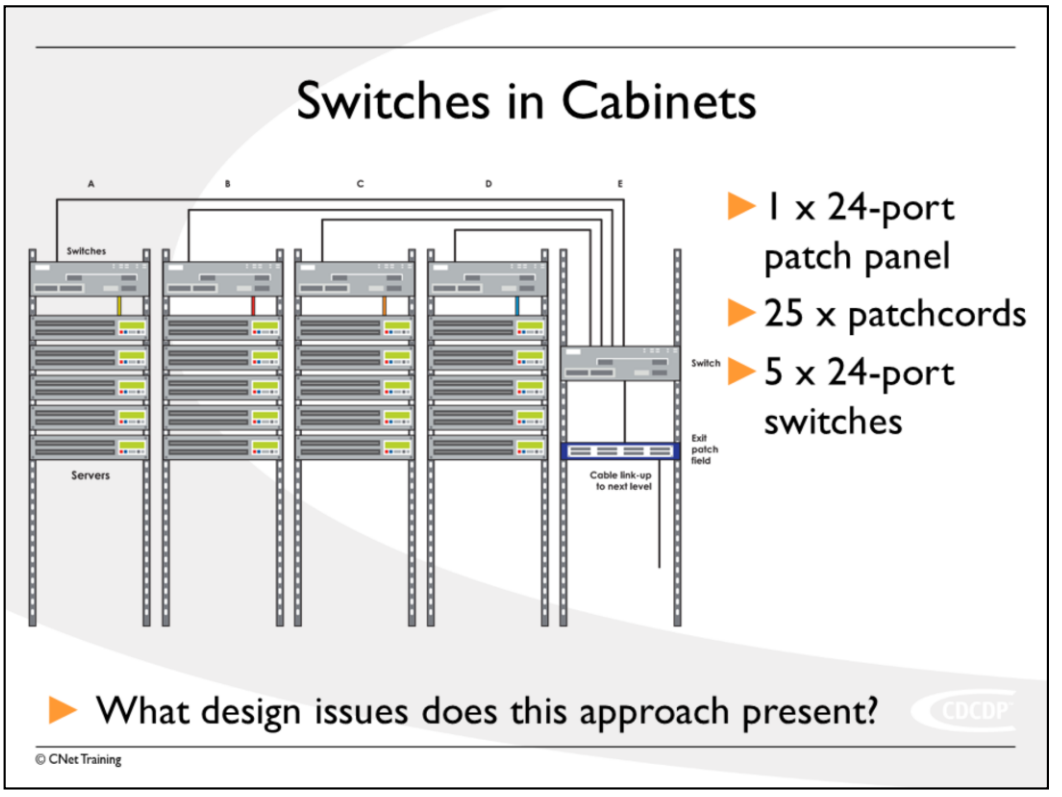


The choice of connectivity is down to the designer, but there are some simple, suggested guidelines to be considered.



Example:

1 panel per rack and all cable back to next level.

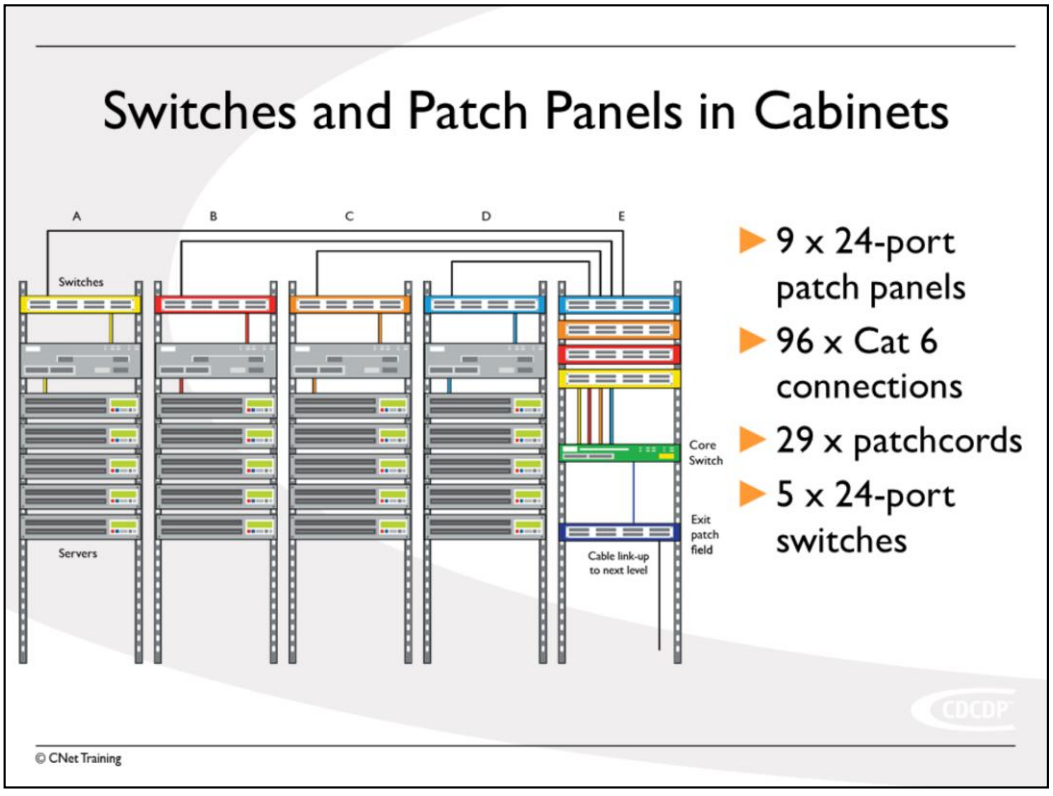


Example:

1 switch per rack

1 aggregate switch per cluster

1 panel per cluster



Example:

1 switch per rack

1 panel per rack

1 aggregate switch per cluster

1 panel per cluster

The quality of the installation work can only be validated by thorough testing to ensure it meets the desired performance specification. There are two specific test criteria:

- Permanent Link Test – The permanent link includes only that portion of the cabling installation that is "permanent" (i.e., the horizontal link from patch panel to patch panel). This is the main test required for cable system warranties.
- Channel Link Test – Defines the performance of the completed end-to-end link as the operating network uses it. The channel test involves everything in the permanent link test, plus the patch cords in the work area, and those used for interconnection and / or cross connection.

It is essential the testing Standards are clearly detailed in the design scope. Failure to do so can (and will) lead to additional installation costs, or a lack of performance capability. All test results must be saved and downloaded:

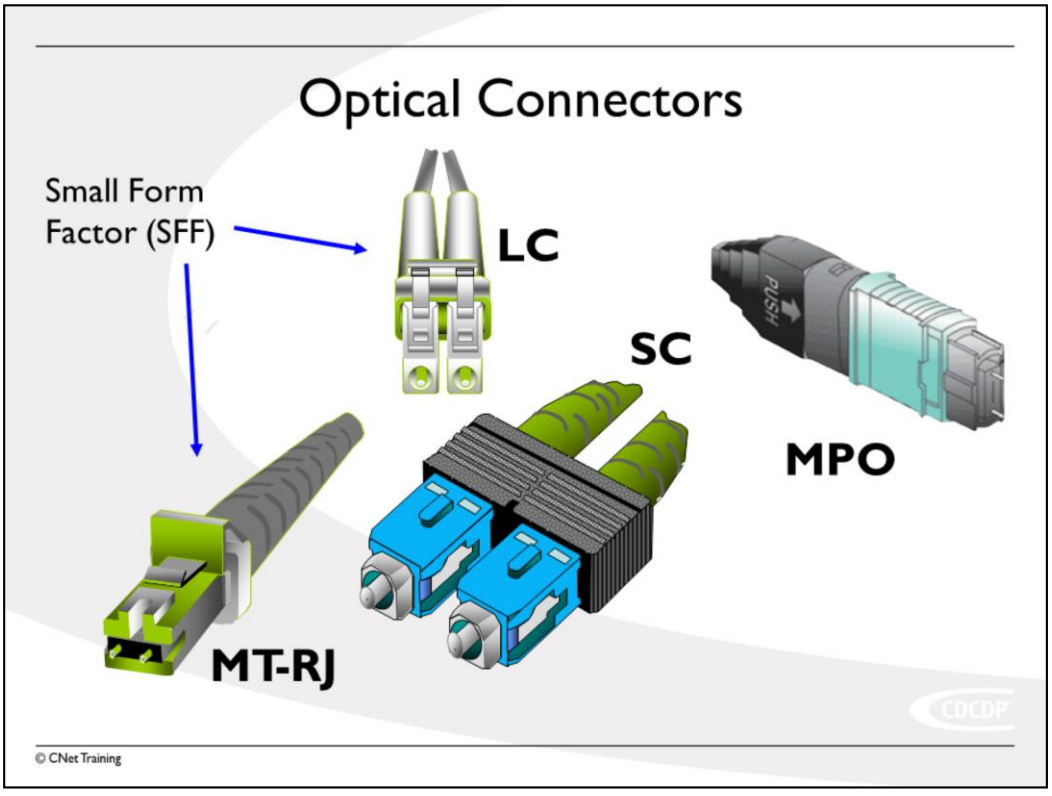
- Copy for customer
- Copy for warranty
- Copy for your own records
- Records must be updated
- Computer-based or paper-based records

Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®)
Core Unit

Optical Fibre Connectivity



These are some of the current connector types.

Cabling Standards specify the duplex SC or duplex LC connector for optical fibre connection points; there are even requirements for a duplex LC APC (angled physical contact) for external network interfaces. For connection of more than two fibres, the MPO connector is required.

They also recognise small form factor (SFF) connectors at other locations, if these meet a certain specification:

- LC: Latching connector
- SC: Subscriber connector
- MT-RJ: Mechanical transfer registered jack
- MPO: Multi-fibre push-on / pull-off connector

Fibre Management

- Supports up to 48 fibres (SFF: MT-RJ and LC)
- Basic fibre management

© CNet Training

Optical fibre needs to be properly managed.

Fibre systems generally terminate in a fibre patch panel.

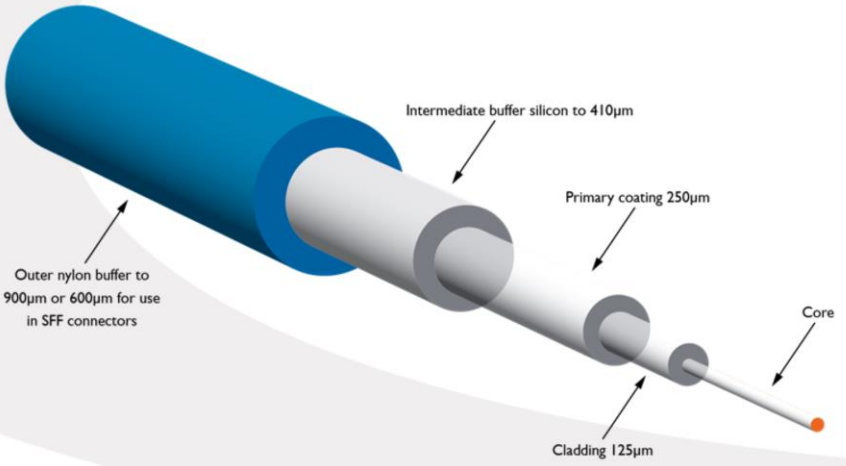
Optical Patchcords

- Optical patchcords can be simplex or duplex
- If duplex, then they do not crossover - i.e., end 'A' to end 'B', and end 'A' to end 'B'

© CNet Training

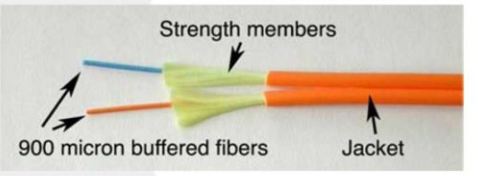
Patchcord specification must match the rest of the fibre network.

Tight-Buffered Optical Fibre Construction

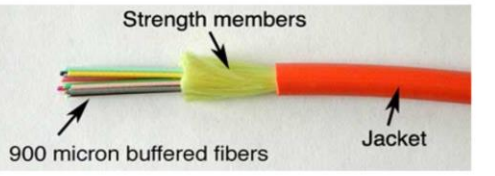


© CNet Training

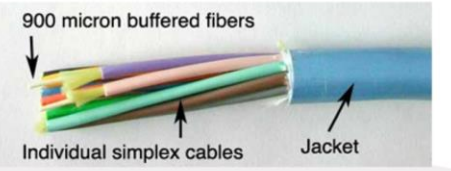
Tight-Buffered Cable Options



- Simplex and zip cord



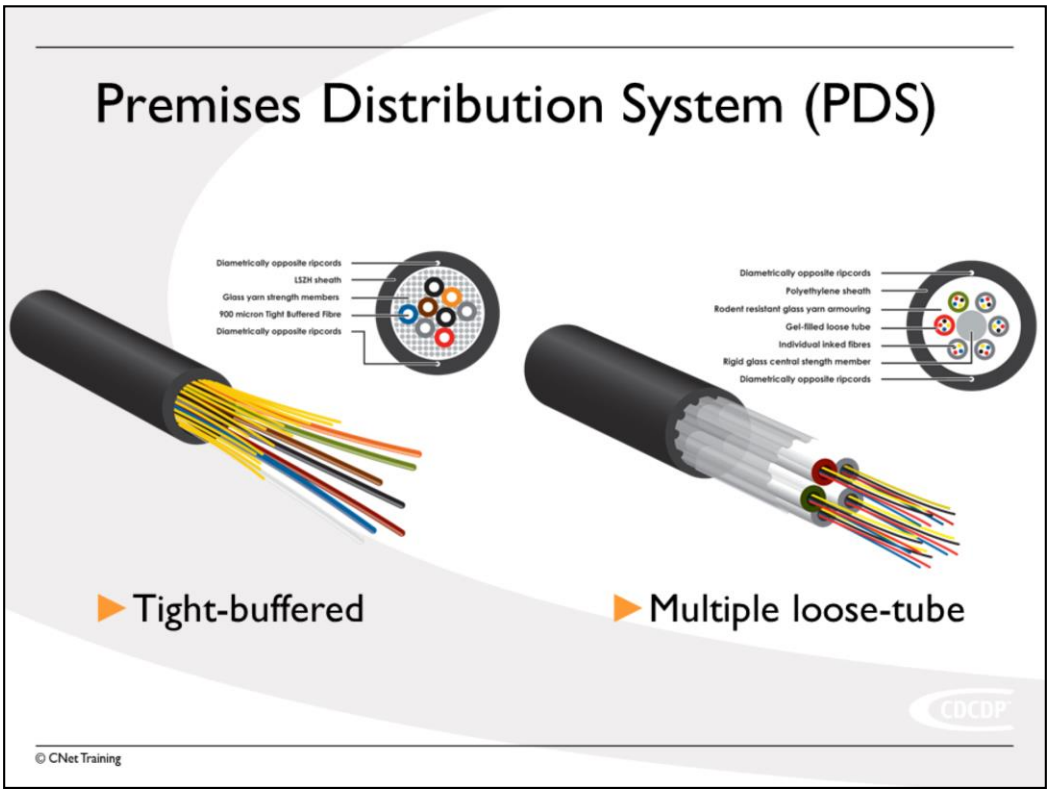
- Distribution cables



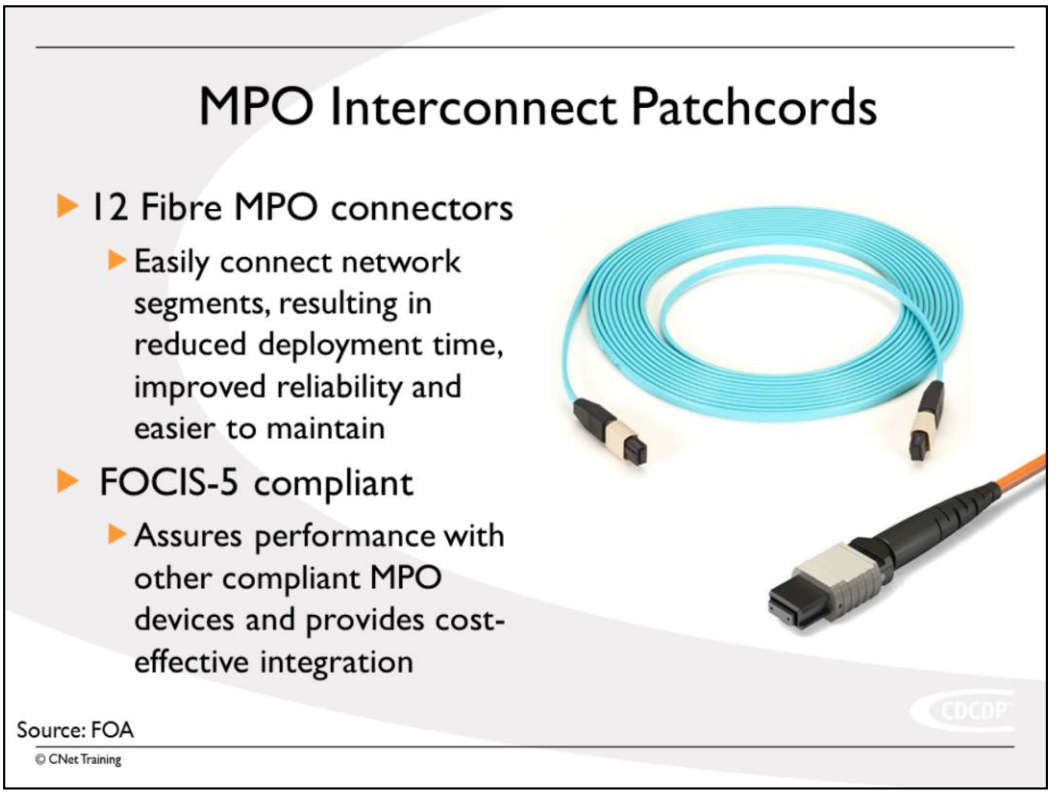
- Breakout cables

Source: FOA

© CNet Training

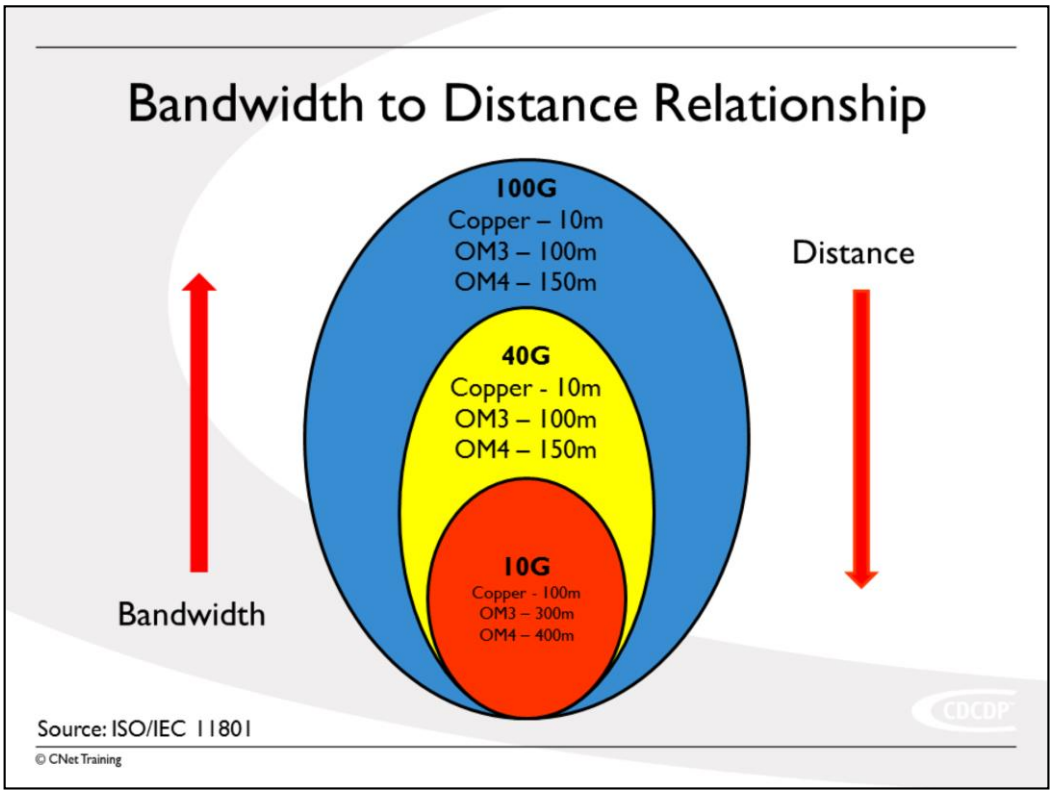


Premise cables provide connectivity from telco providers, or between campus buildings. Type and construction of premise distribution cables need to be fully appreciated, as local regulations dictate they should be spliced to internal structured cables within 15m of the building entrance facility / demarcation.



MPO connectors are allowed by the Standards, providing that they meet designated requirements of the Fibre Optic Connector Intermateability Standards (FOCIS).

- **MPO:** Multi-fibre, push-on / pull-off
- **MTP:** Multi-fibre termination / push-on



Copper cables reach their 10G Ethernet limit at around 100m (328ft). Beyond that, optical fibre is needed. That said, even with multimode fibre, distance capabilities will reduce in proportion to the bandwidth increase. This is a key factor that must be understood during the design phase in accordance with bandwidth and growth projections.

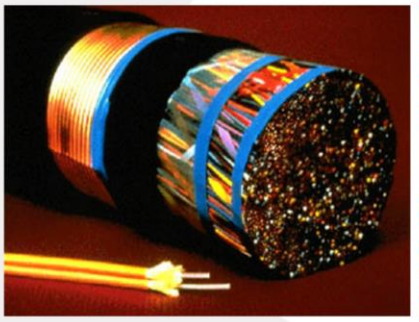
Copper or Fibre?

- For transmission distances in excess of 100m (328ft), the answer can only really be optical fibre
- For distances less than 100m (328ft), we have to consider the merits of fibre versus copper, and the relative costs of each technology

© CNet Training

The discussion on choice between copper and fibre is only relevant at short distances.

Optical Fibre Benefits



- Immune to electrical interference
- Secure and does not radiate energy
- Carries minimal power, so cannot be a source of ignition
- Very high bandwidth
- Low attenuation + long runs
- Smaller and lighter than copper equivalent
- Optical equipment consumes less power
- Cheaper to run and less heat generated

© CNet Training

Optical fibre has some significant advantages.

Potential Optical Fibre Drawbacks

- Limitations with power and voice over IP (VoIP)
- Still more expensive under 100m (328 ft)
- Overall running costs may be lower

Copper

Rate Mbps	Active Link Power (W)
10	0.63
100	1.14
1000	3.9
10000	10

Fibre

3–5 W for most fibre technologies

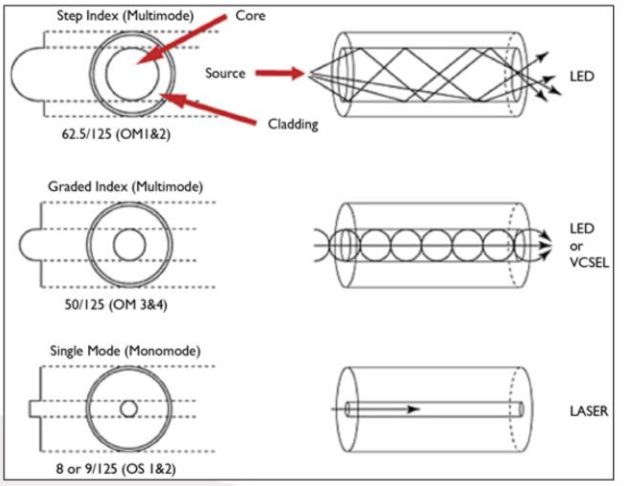
= £2 per copper 10GBASE-T link per year excess over fibre, 5000 links = £10k per year extra electricity + £10k year air conditioning

© CNet Training

But it is not as simple as that - There are numerous design considerations requiring proper assessment, in line with present and future business demands.

Fibre Transmission Characteristics

- Make-up of the fibre construction: Plastic or glass, or a combination of both
- Launch equipment: From a basic LED to high-end, quality LASER



LASER - Light amplification by stimulated emission of radiation
VCSEL - Vertical cavity surface emitting laser
LED - Light emitting diode

© CNet Training

Number before '/' indicates the core size and the number after denotes cladding size.

ISO 11801 and CENELEC EN 50173-1

Category	Maximum attenuation (dB/km)		Minimum Modal Bandwidth (MHz.km)		
			Over-filled launch bandwidth		Laser launch bandwidth
	850nm	1300nm	850nm	1300nm	850nm
OM1	3.5	1.5	200	500	Not specified
OM2	3.5	1.5	500	500	Not specified
OM3	3.5	1.5	1500	500	2000
OM4	3.5	1.5	3500	500	4700

© CNet Training

Current Standards now include OM4.

The figures shown in the table above are the 'worst case' allowed in order to comply with the Standard. The parameters for the real fibre used in a typical installation will show much better performance than this - for example, 2.5dB at 850nm for the OM3 case.

Link Loss by Application

Application	Wavelength	dB Loss
10BASE-FL	850	10
100BASE-F	1300	11
1000BASE-SX	850	2.38 / 3.37
1000BASE-LX	1300	2.35 / 2.35
Fibre Channel SX	850	6
Fibre Channel LX	1300	9.5
ATM155	1300	7
ATM622	1300	6
ATM155 SWL	850	7.2
Token Ring	850	13
10GBASE SR/SW	850	2.6

© CNet Training

Different applications have upper limits for end-to-end losses in the system. They will successfully operate if these limits are not surpassed.

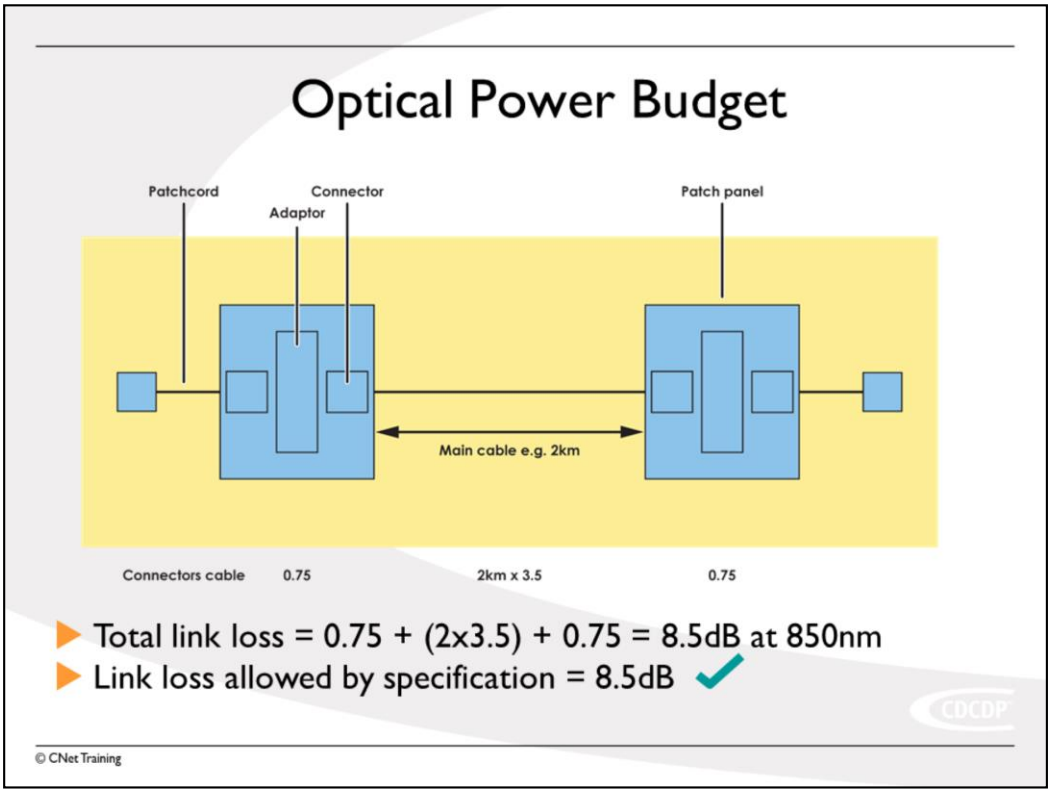
Fibre Application Distances

Fibre Grade	100BASE-FX	1GBASE-SX	1GBASE-LX	10GBASE-SR	10GBASE-LX	1Gb FC	2Gb FC	4Gb FC
OM1	2000m (1.24 miles)	275m (900')	550m (1804')	32m (105')	300m (984')	N/A	N/A	N/A
OM2	2000m (1.24 miles)	550m (1804')	550m (1804')	82m (270')	300m (984')	300m (984')	150m (492')	N/A
OM3	2000m (1.24 miles)	550m (1804')	550m (1804')	300m (984')	300m (984')	500m (1640')	300m (984')	300m (984')
OM4	2000m (1.24 miles)	550m (1804')	550m (1804')	400m (1312')	400m (1312')	500m (1640')	300m (984')	300m (984')
OSI	2000m (1.24 miles)	-	2000m (1.24 miles)	-	2000m (1.24 miles)	2000m (1.24 miles)	2000m (1.24 miles)	2000m (1.24 miles)
OS2	2000m (1.24 miles)	-	5000m (3.1 miles)	-	10000 (6.2 miles)	2000m (1.24 miles)	2000m (1.24 miles)	2000m (1.24 miles)

Source: EN 50173-1

© CNet Training

This table demonstrates the distances possible using different grades of fibre. In practice, longer distances are possible, particularly on singlemode fibre, where higher power launch can be used to overcome attenuation.



The power budget is key to system performance and needs to be accurately calculated during the design phase.

How Many Connectors Can We Have in the Channel?

- OM3 fibre has sufficient bandwidth for 300m (984ft 3 in) transmission and a loss budget of 2.55dB
- Presume that the fibre attenuation is 3.5 x 0.3 = 1.05 - this leaves 1.5dB for connecting hardware
- Taking the Standards-based allowance of 0.75dB per connection and dividing into 1.5, we get the answer of two
- No splice
- Connector loss allowance:
  - 100% bt 0.75dB / 95% bt 0.5dB / 50% bt 0.35dB

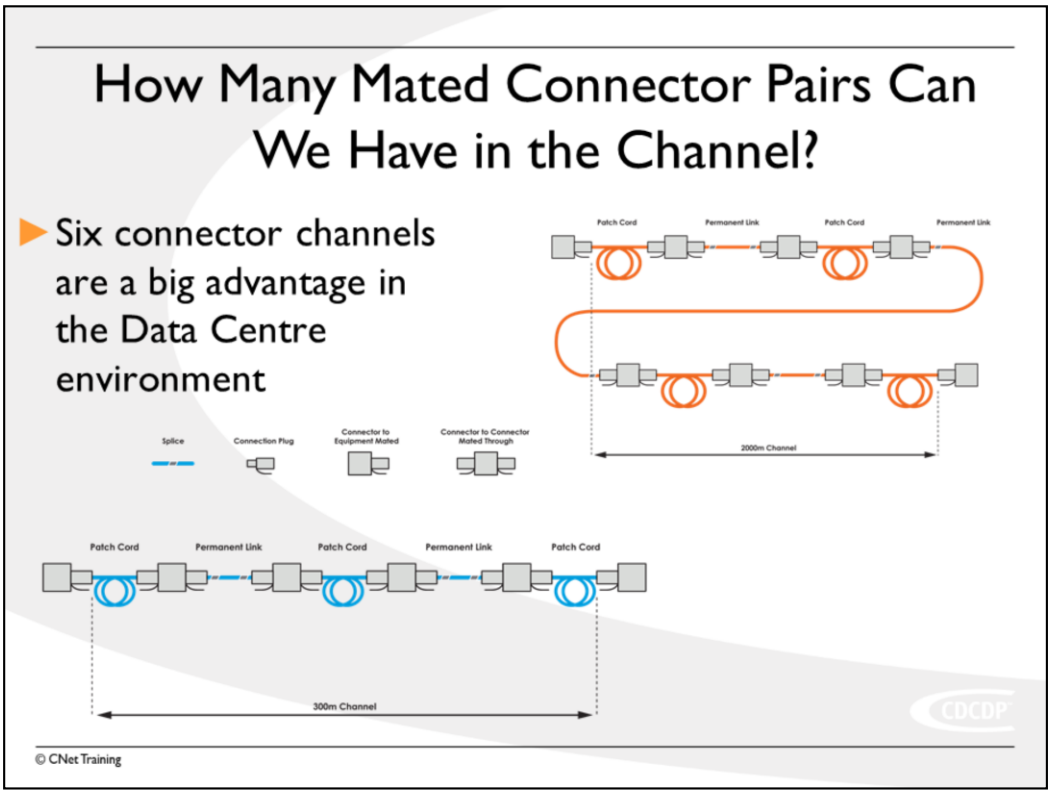
© CNet Training

IEC mandates 50% better than 0.35dB.

Maximum Possible Number of Connectors in a Premium OM3/4 Channel

- Using a 0.3dB premium LC connector (factory terminated) and best loss fibre, the answer could be as high as six points of interconnection
- Manufacturers would not recommend more than six

© CNet Training



Six connectors fit with the Data Centre design topologies.

Design Choice Considerations

- Determine applications and distances required:
  - Future Proof?
    - Next generation applications have tighter limits and shorter reach
    - 40G /100G on multimode?
  - Over 300m (984ft) and greater than 2.55dB:
    - Install singlemode, OS1 or OS2
  - Under 300m (984ft 3in):
    - Install OM3 or OM4
  - Calculate number of connections using rules already explained

© CNet Training

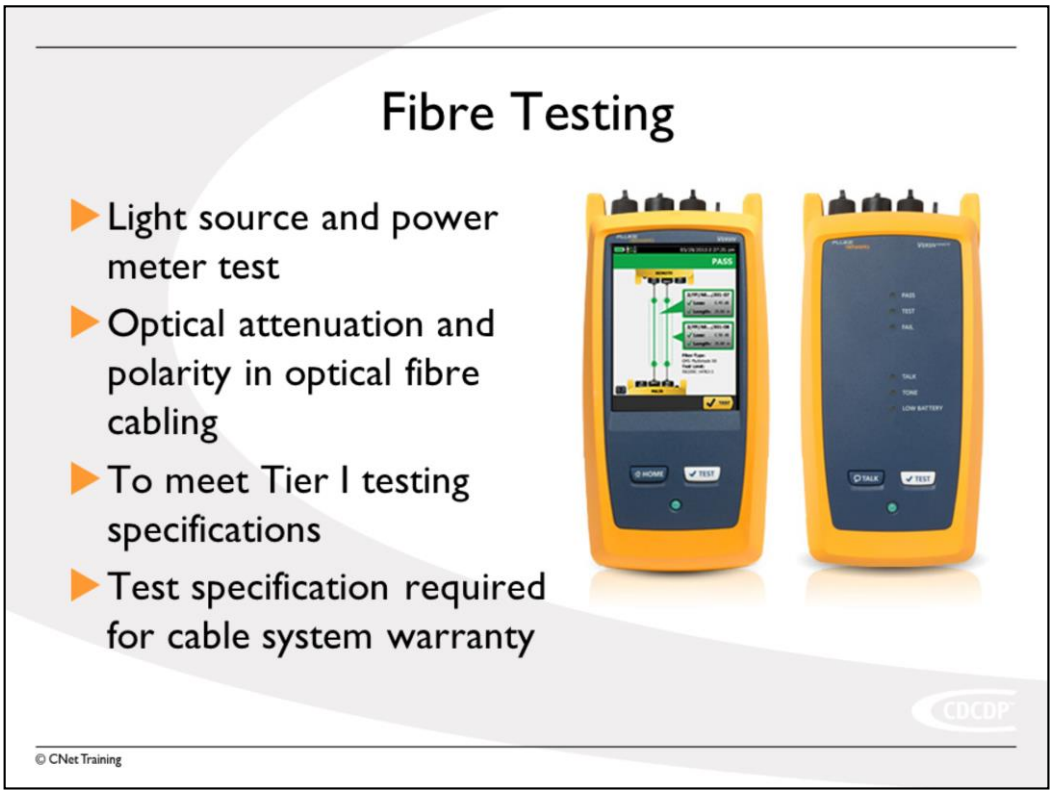
Design for Growth Management

- Data Centres are not static - it is impossible to guess on Day One how they will develop, so a flexible approach is needed
  - Appreciate the bandwidth to distance limitations
  - Check the number of connectors and splices in the channel
  - Additional fibre deployment needs to be fast and can ideally take place in normal working hours
  - Use quality cabling of the same category and fibre type
  - Test in accordance with the relevant Standards
  - Redundant fibre should be easily recovered

CDCDP

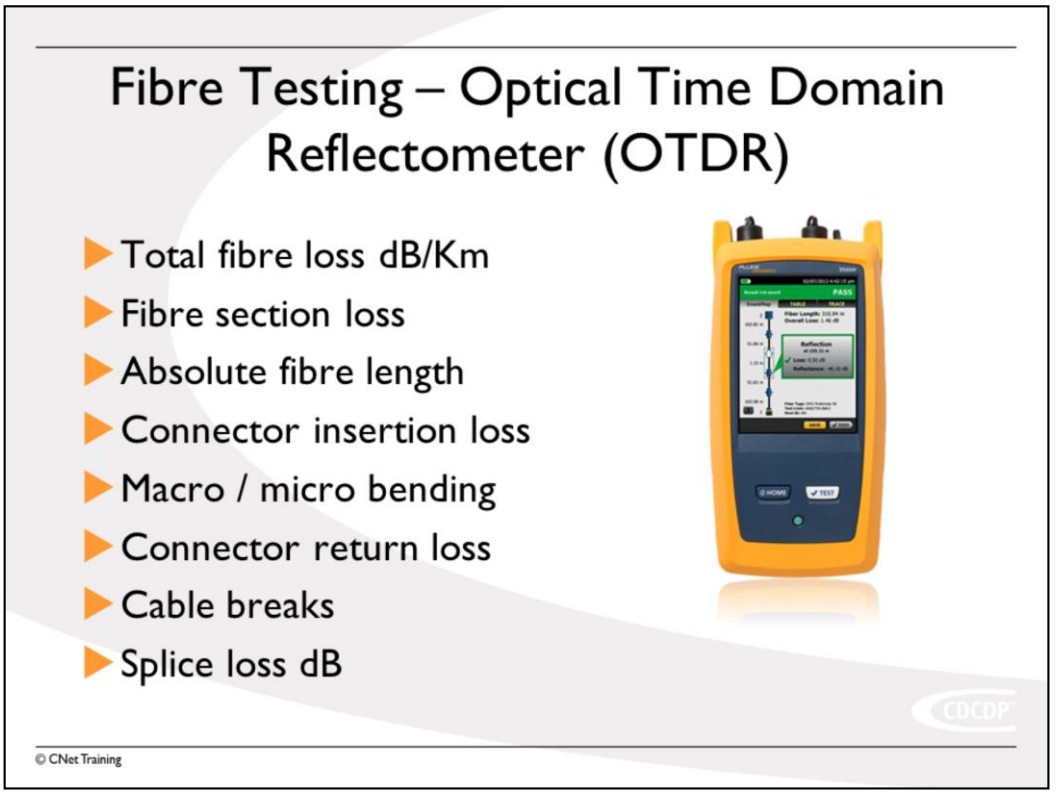
© CNet Training

Designers should manage the growth of the facility from Day One and anticipate the capacity requirements of connectivity, containment, power and cooling. This affords a modular growth principle, minimising capital investment to an 'on demand' approach. Although this approach generally offers no timescale advantage to the original deployment, subsequent requirements can be satisfied by rapid deployment of fibre, utilising the infrastructure established Day One; this can provide significant cost savings in overall installation man-hours on subsequent installations, especially when the infrastructure is under raised access floors that can only be accessed out of normal working hours.



TSB-140 provides descriptions for two tiers of optical fibre test measurement methods and describes field-testing of length, optical attenuation and polarity in optical fibre cabling, using an optical loss test set (OLTS), optical time domain reflectometer (OTDR) and a visible light source, such as a visual fault locator (VFL).

- Tier 1 testing entails measuring installed optical fibre cabling for attenuation with an optical loss test set (OLTS) and polarity.
- Tier 2 testing (which is optional) includes the Tier 1 validation, plus the addition of an optical time domain reflectometer (OTDR) trace. An OTDR can be used to characterise the installed fibre link, indicating the uniformity of cable attenuation and connector insertion loss.



Optical Time Domain Reflectometers (OTDRs) measure the amount of backscattered light from the optical fibre under test, and therefore produce a 'footprint' of the installed optical fibre, thus producing a value for attenuation of the fibre, usually expressed in dB/km and the length of the fibre. For this reason, the OTDR is a very useful tool for troubleshooting and for verifying the installation of optical cabling. Splice loss measurements can be made, as well as analysis of either: A) Sections of an installed cable or, B) An overview of the complete end-to-end link.

Reasons for using a OTDR?

- Single-ended test of a link
- The total length can be detected
- The quality of installation can be verified and improved
- Each individual segment can be evaluated
- A trace represents the entire link
- Build a knowledge base for an installed plant
- Complete documentation
- A source of later variation / degradation can be identified
- The only way to efficiently troubleshoot an installed link or channel

Any Questions?

© CNet Training

Certified Data Centre Design (CDCD®)
Core Unit

Pre-terminated Cables

Pre-terminated Cabling Solutions

- Copper and fibre optic cabling can be connectorised offsite, leading to:
  - Reduced time onsite - up to 75% less
  - Increased quality and consistency
  - Reduced onsite supervision levels required, due to simplicity of the installation
  - Reducing skill shortfall risk to virtually zero, as there is potentially little need for sub-contract labour
  - Virtually zero onsite fault correction rate
  - Skilled workforce operating in conditions conducive to total quality manufacturing
  - Repeatable, high-quality terminations with a consistent performance across all ports
- Terminated in individual connectors or cassettes
- Terminated at both ends or just one end

© CNet Training

Pre-terminated cable solutions are becoming popular and offer some advantages. Onsite time is reduced, but careful planning and design is key to making it successful. Here are a few points to consider:

- Reducing skill shortfall risk to virtually zero, as there is potentially little need for subcontract labour
- Virtually zero onsite fault correction rate
- Skilled workforce operating in conditions conducive to total quality manufacturing
- Repeatable, high-quality terminations with consistent performance across all ports
- Not all installers accept it because it shifts value to the manufacturer
- Much more time must be spent accurately surveying cable routes
- Not all cabling copes well with the pre-terminated bundling process
- Cable must be 100% tested in the factory and usually sample-tested after installation
- Systems are manufactured by both original cabling manufacturers and installers

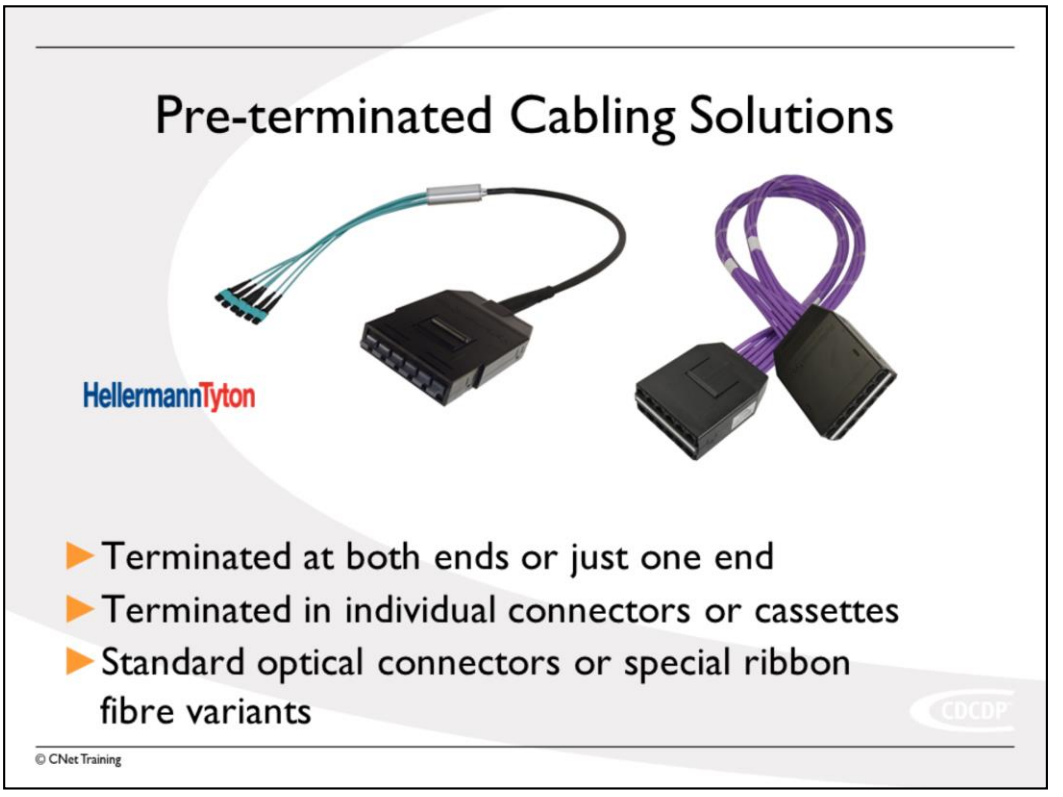
Pre-terminated Cabling Solutions

- However:
  - Not all installers accept it because it shifts value to the manufacturer
  - Much more time must be spent in accurate surveying of cable routes
  - Not all cabling copes well with the pre-terminated bundling process (more specifically, copper applications)
  - Cable must be 100% tested in the factory and usually sample tested after installation

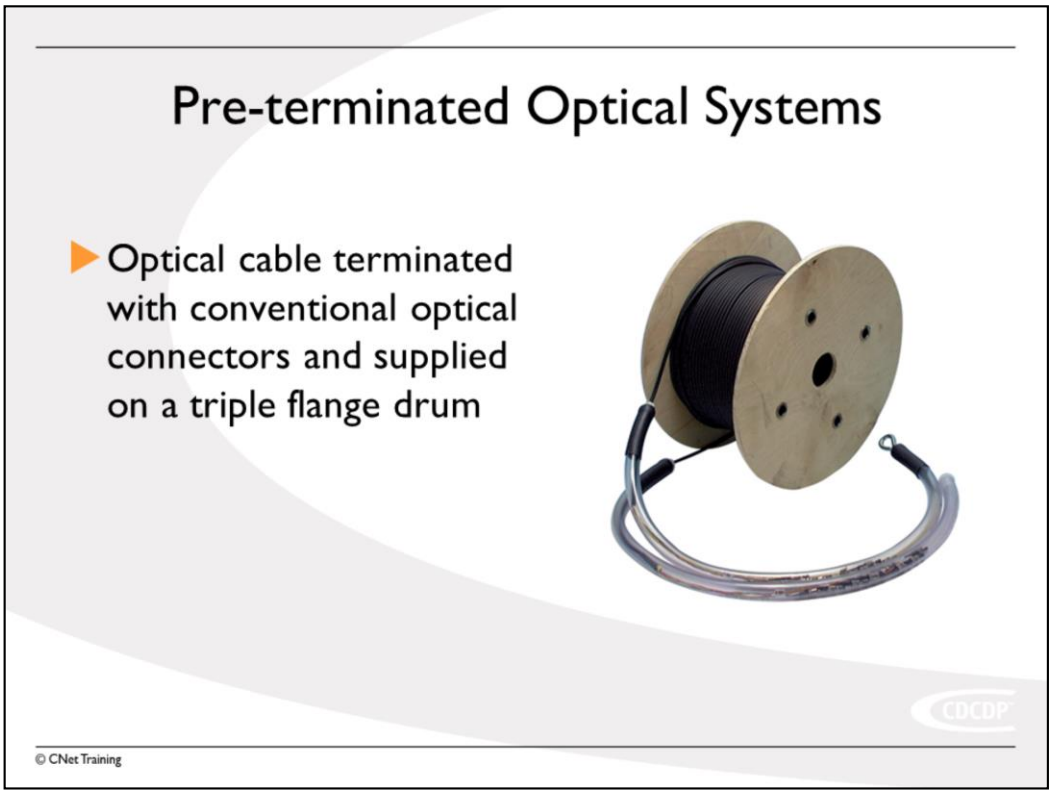
© CNet Training

Not all installers are capable of dealing with pre-terminated solutions, therefore there is resistance, and this is a factor the CDCD must consider.

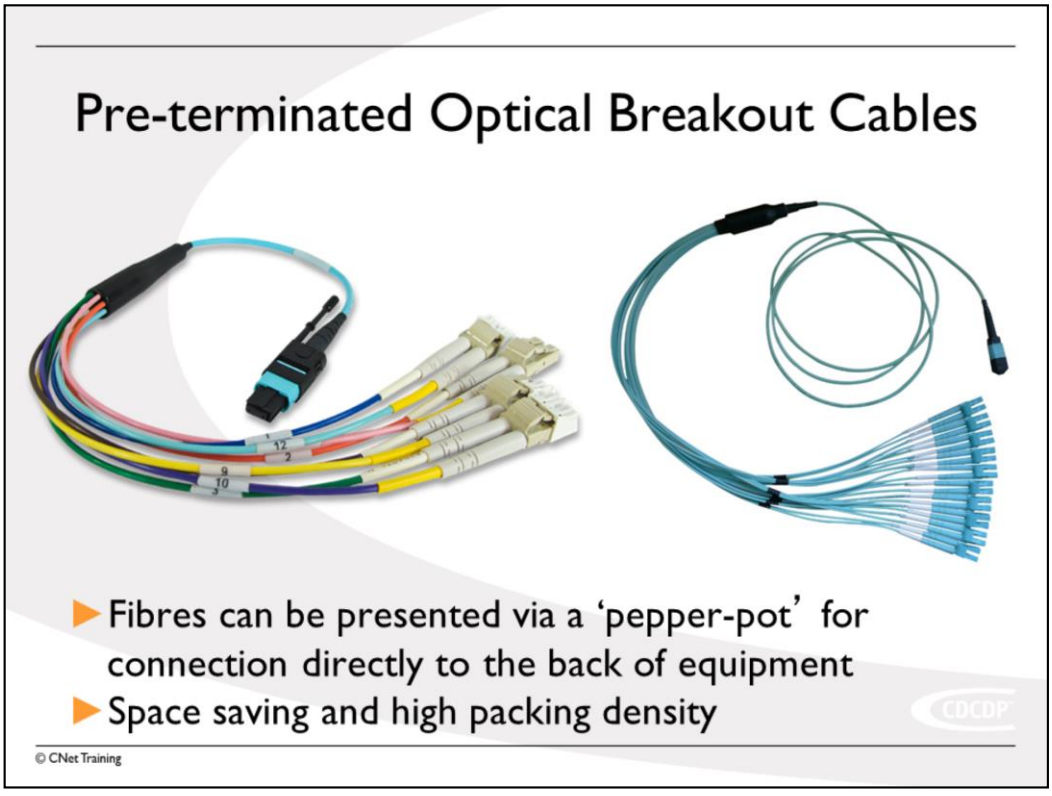
It is always a good idea for the CDCD to prepare and hand over all test results and graphs as part of the specification responsibilities of the installer and commissioner.



There are several solutions, and the CDCD must choose the relevant option for the Data Centre requirement.



Pre-terminated fibre optical cables are stored on special drums, which assist with installation.



Pre-terminated fibre optic breakout cables can be presented with the appropriate length tails and connectors, so they connect directly to the equipment without the need for a patch panel. This reduces connector count and improves the optical budget.

Review

- Can you?
  - Identify some copper and optical fibre component options
  - Identify some of the copper and optical and copper design options
  - Identify their operational suitability
  - Discuss which option to choose

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 7

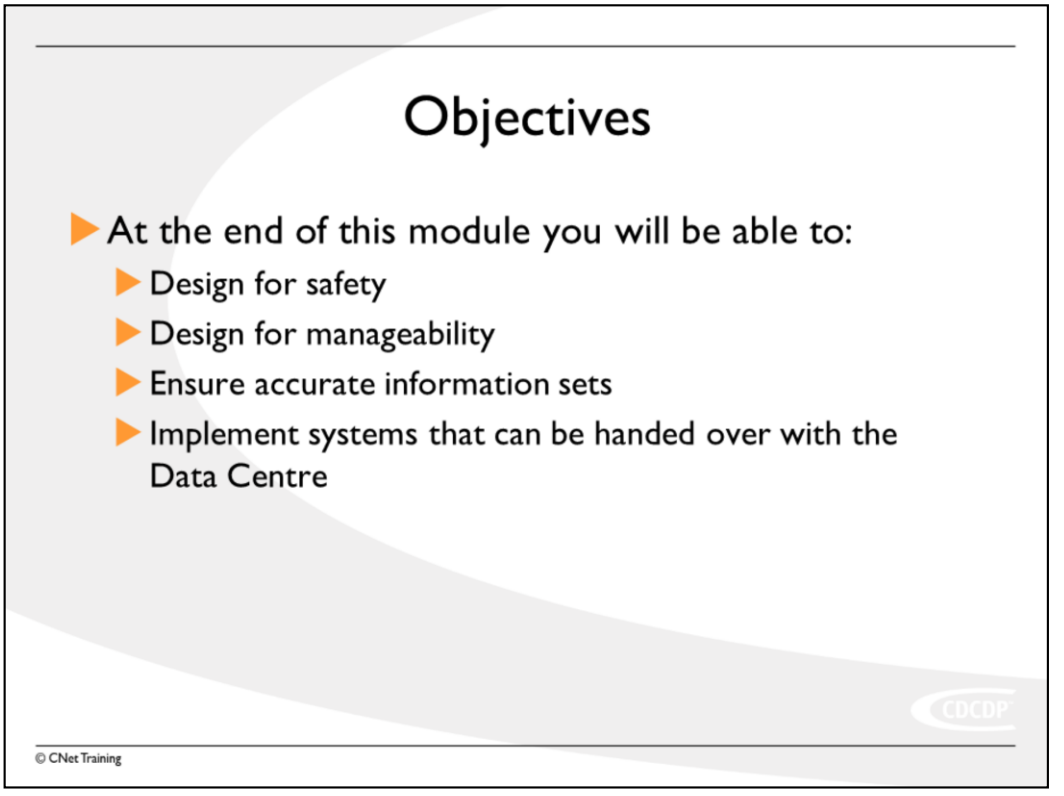
© CNet Training

Certified Data Centre Design (CDCD®) Core Unit

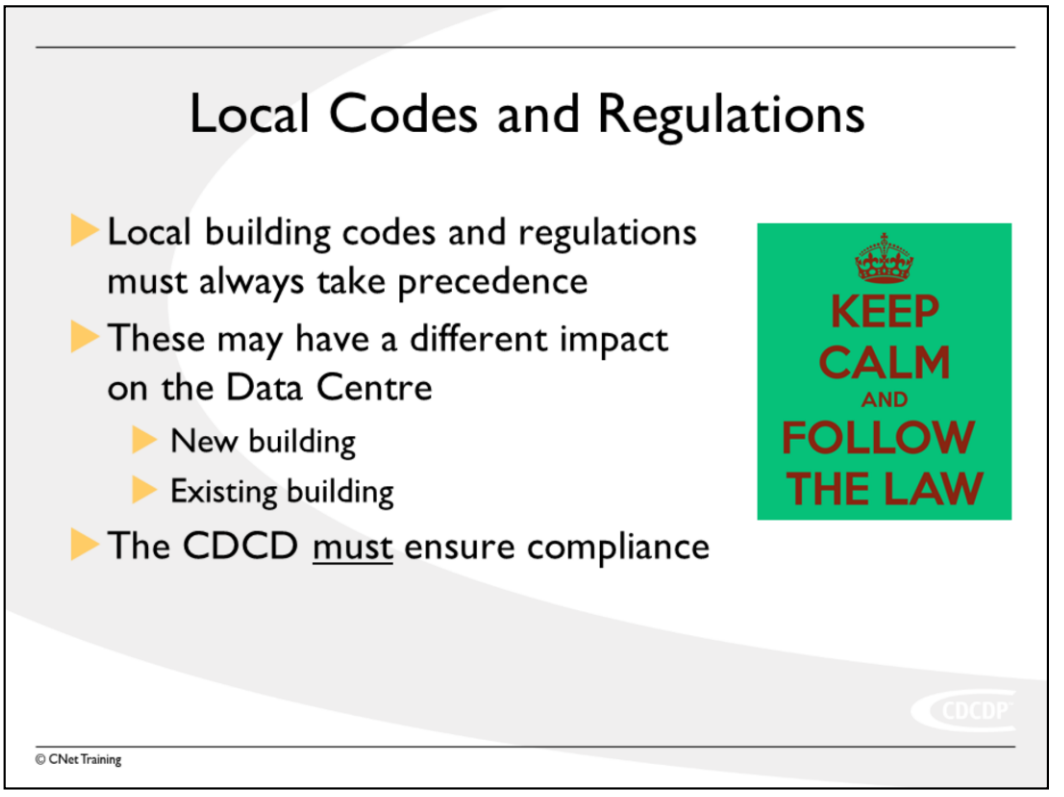
Designing for Safety and Manageability

Version 1509

CDCDP

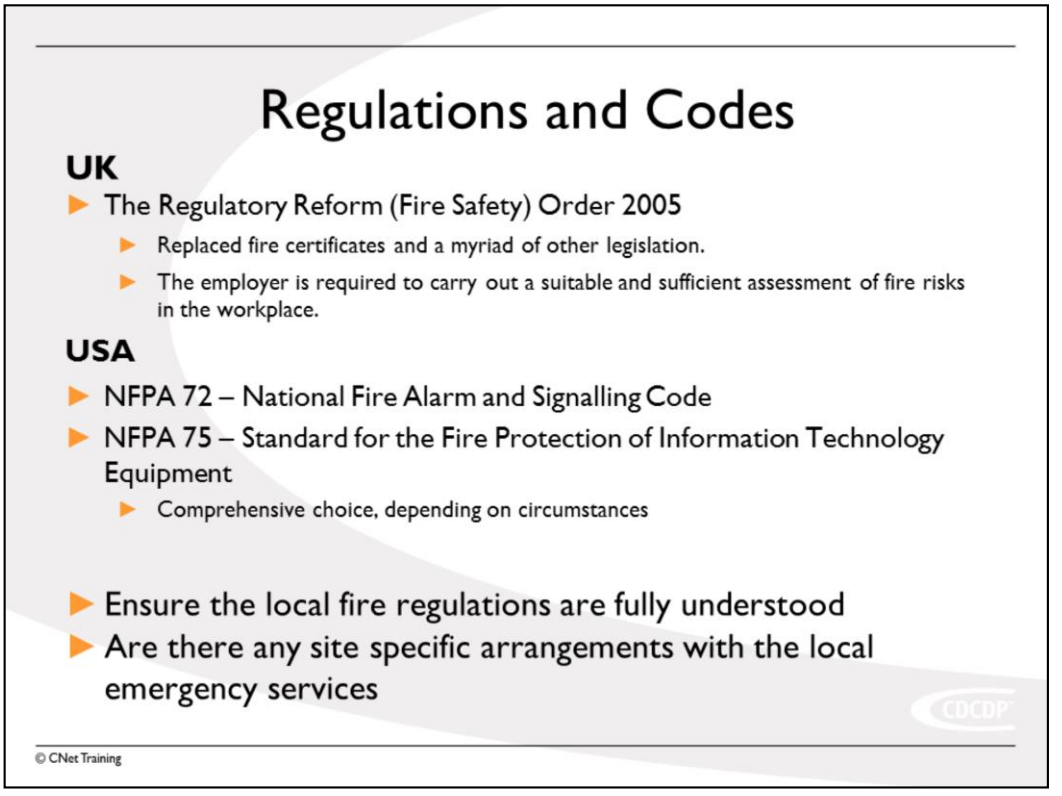


The CDCD must appreciate the operator has to live with the Data Centre design for some years, and therefore must consider longterm manageability as a key factor.



The building chosen as the Data Centre site can affect, and severely limit what can be achieved by the design.

The CDCD must confer with the local building authorities and understand what options are available at the earliest stage of the design project.



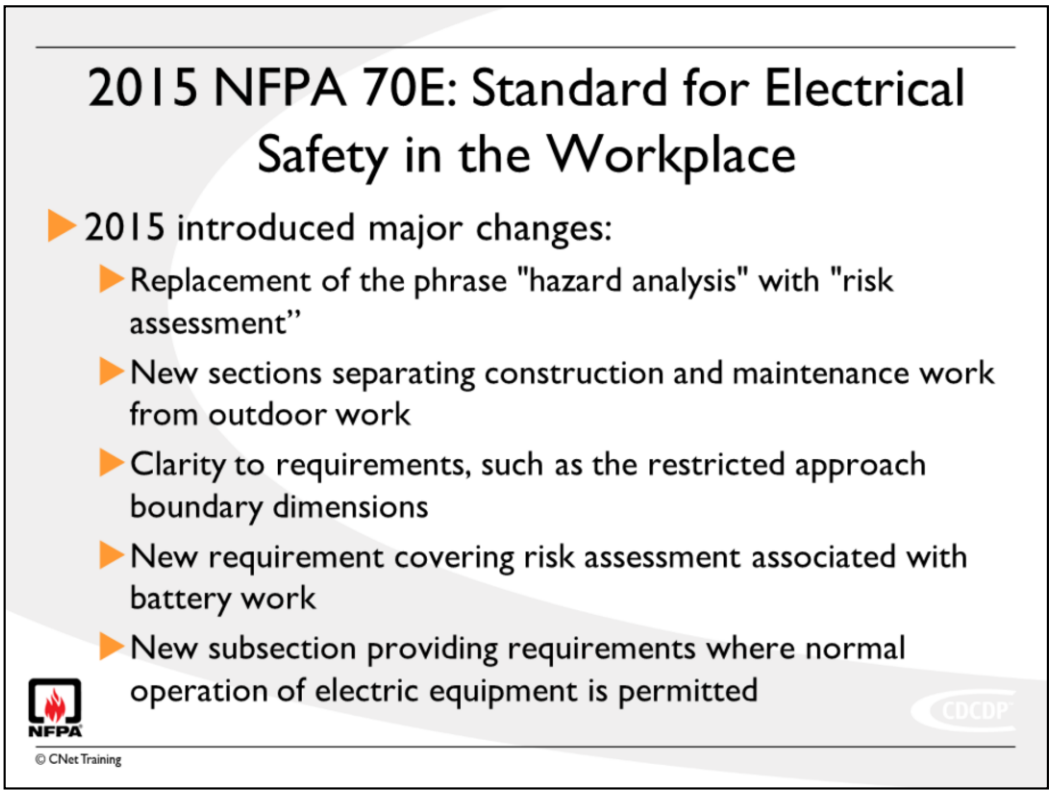
In the UK, changes have been made to legislation, including the responsibilities of building owners / occupiers / employers.

The risk assessment must be quite detailed to cover all eventualities.

- Ignition hazards
- Combustible materials hazard
- Persons at risk
- Contractors
- Fire detection and warning
- Firefighting equipment
- Means of escape
- Management structure
- Training and evacuation exercises
- Tests and maintenance
- Records
- Obligations to inform or consult others

In the US, requirements are dealt with by a comprehensive set of NFPA Codes.

Other countries have their own regulations.



The 2015 edition of NFPA 70E introduces a major change in how stakeholders evaluate electrical risk, so owners, managers, and employees can work together to ensure an electrically safe work area, complying with OSHA 1910 Subpart S and OSHA 1926 Subpart K.

- Key changes throughout the Standard replace the phrase "hazard analysis" with "risk assessment" to enable a shift in awareness about the potential for failure.
- Revisions enhance usability, such as the division of requirements separating construction and maintenance work from outdoor work.
- Updated tables add clarity to requirements, such as the restricted approach boundary dimensions.
- New requirement covering risk assessment associated with battery work.
- New subsection providing requirements where normal operation of electric equipment is permitted.
- Informative Annex E has updated text to correlate the redefined terminology associated with hazard and risk. This annex provides clarity and consistency about definitions as well as risk management principles vital to electrical safety.

Fire Safety Plan

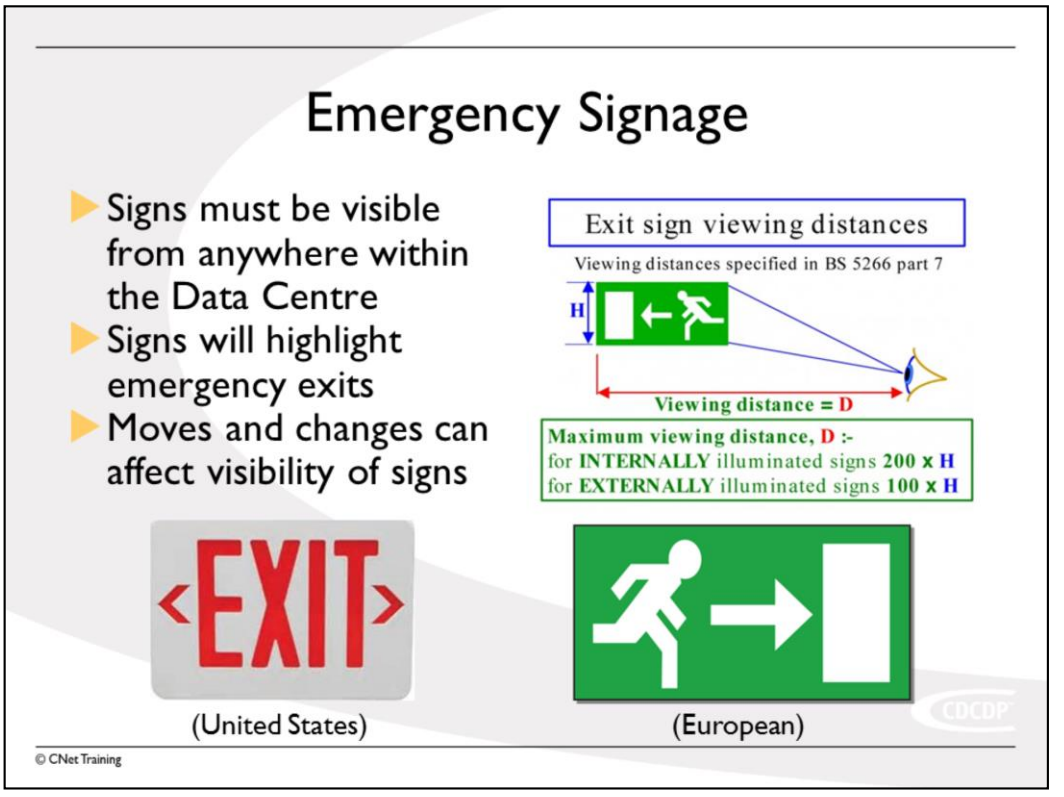
- The fire safety plan is a multi-layered approach that requires a coordinated outline for:
  - Designing for low flammability and fire risk
  - Operating with low risk
  - Emergency exits
  - Emergency lighting
  - Emergency exit signage
  - Fire detection, appropriate to the area covered
  - Fire alarms
  - Multilevel automatic fire suppression
  - Manual fire alarm and portable fire extinguishers
  - Staff training and fire drills
  - Maintenance plan for all equipment

CDCDP

© CNet Training

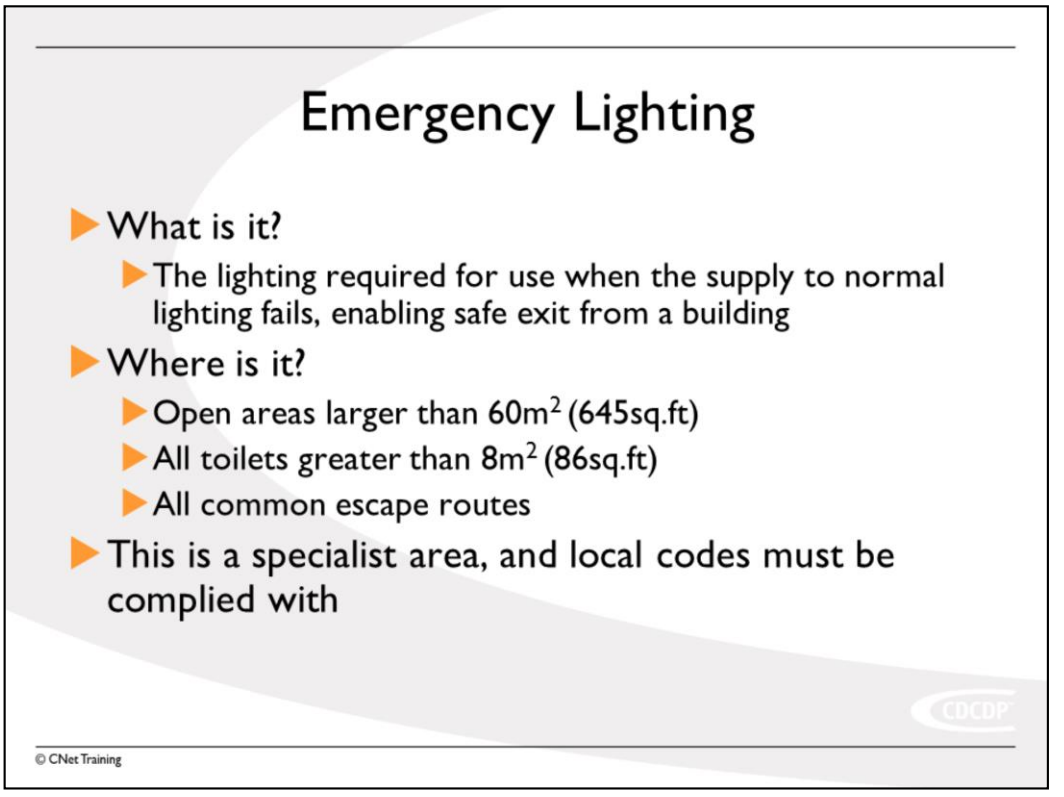
It is important the Data Centre design does not compromise the fire safety aspects of the building. Regulatory requirements are quite strict and need to be carefully considered throughout the design and implementation process. There is no ABC of fire safety - the issue must be considered holistically:

- What are we protecting?
- What are we protecting against?
- How do we control it?
- How do we stop it?



Other regulations and Standards must be maintained, such as those covering emergency situations. These vary between countries, and therefore local codes and regulations must be taken into account; consult the local Authority Having Jurisdiction (AHJ).

Signs showing the emergency exit routes must be visible around the Data Centre. This is an area that must be considered - does the new equipment obstruct the view? Many Data Centres have fallen afoul of this. It is not normally the responsibility of the CDCD to specify the emergency systems, as he / she will consult a specialist.



The first question is: What is emergency lighting?

It is lighting required when normal lighting fails, thus enabling safe exit from a building.

Building codes and regulations vary between countries, and it is important to consult the applicable ones. Most regulations state certain areas should have emergency lighting.

In a Data Centre, these include:

- Open areas larger than 60m^2 (645 sq.ft) in area (e.g., the computer room)
- All toilets greater than 8m^2 (86 sq.ft) in area
- All common escape routes

Codes of practice lay down minimum illumination levels in escape routes and open areas. Codes of practice also lay down requirements governing siting of emergency lighting fixtures; for example, the UK code of practice, BS5266, specifies a fitting must be within 2 metres (6ft 7in) horizontal distance of a fire alarm call point, or location for fire fighting appliances

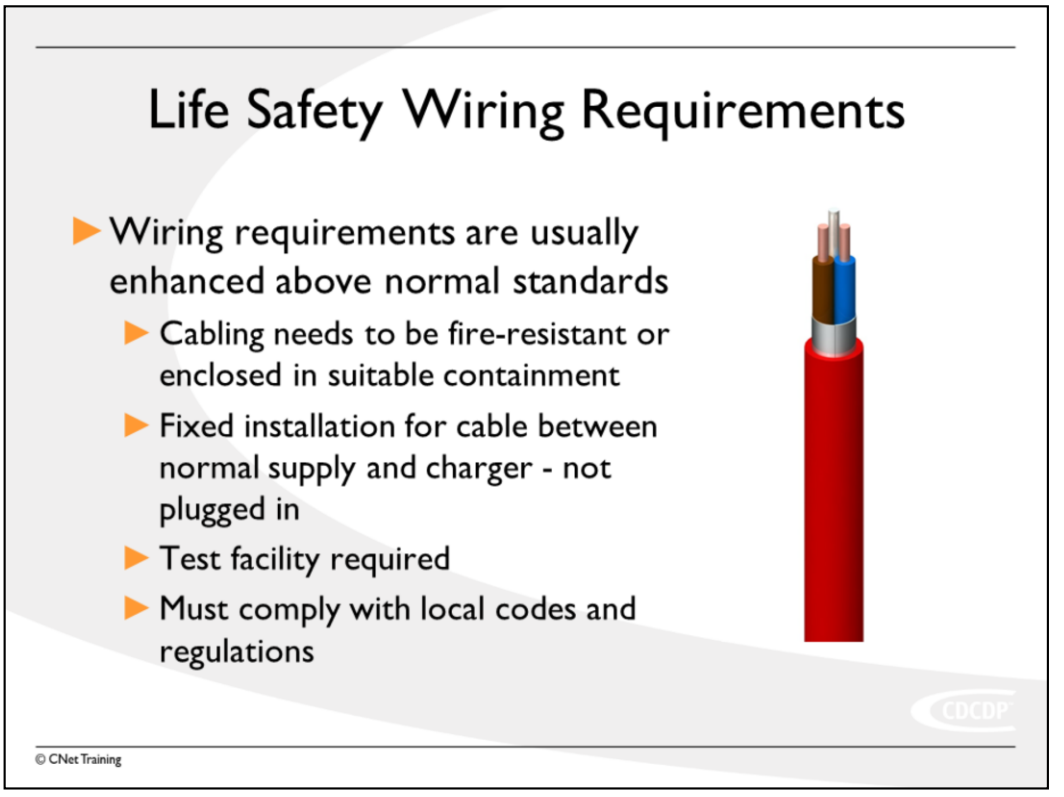
Emergency Power Systems

- An independent energy supply for essential safety equipment using batteries as the alternative power source

© CNet Training

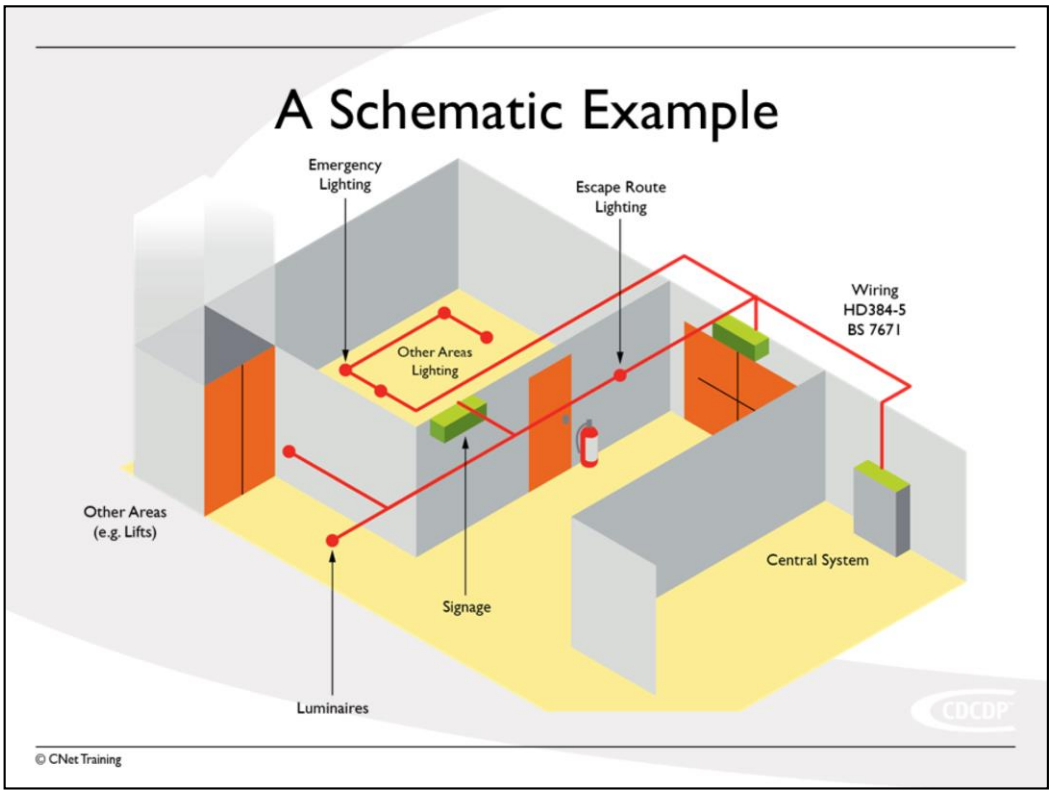
Centrally-supplied emergency power systems have specific regulations and Standards that must be maintained.

This is a separate requirement to the standby power for critical IT equipment.



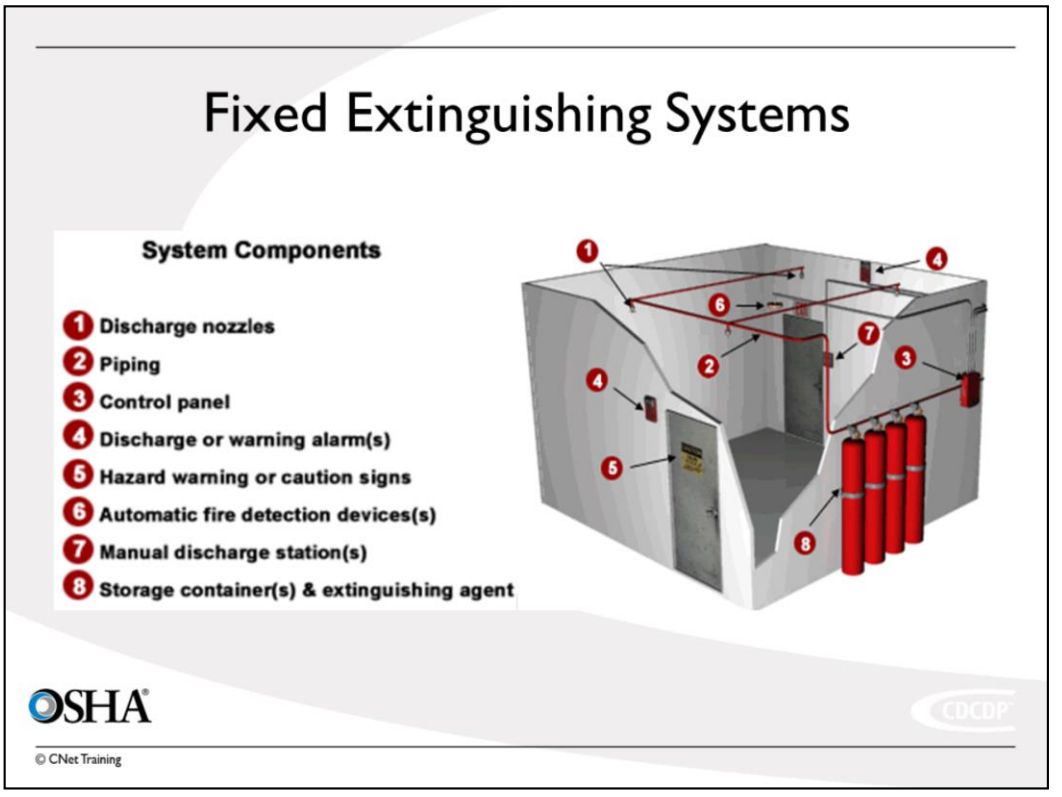
Similarly, the wiring Standards for emergency systems are in addition to normal wiring regulations.

The CDCD must ensure local codes are applied.

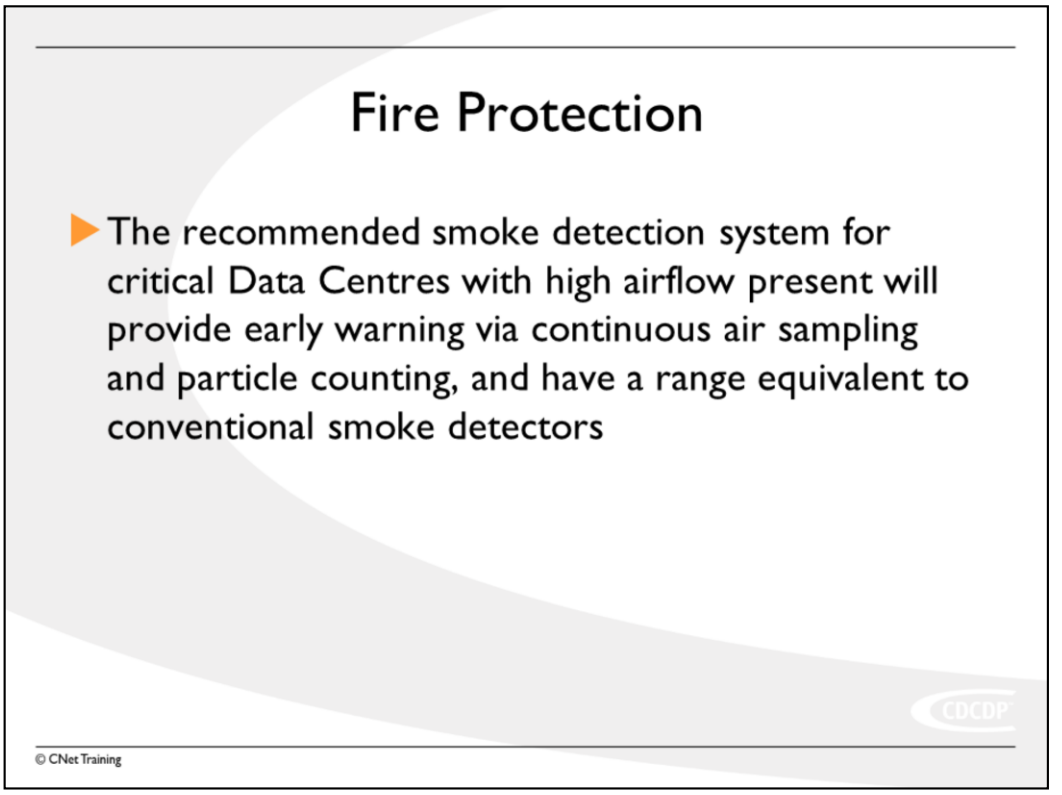


A schematic example showing the principles is shown above.

In any jurisdiction, there may be additional Standards which must be taken into account. This is a specialised area the CDCD needs to be aware of, so they can liaise successfully with the specialists.



Fixed fire extinguishing and suppression systems are commonly used to protect areas containing valuable or critical equipment, such as data processing rooms, telecommunications switches, and process control rooms. Their main function is to quickly extinguish a developing fire and alert occupants before extensive damage occurs, by filling the protected area with a gas or chemical extinguishing agent.



USA

For instance, TIA 942-A recommends three systems:

- One system would be at the ceiling levels of the computer room, entrance facilities, electrical room, and mechanical rooms, as well as the intake to the computer room air-handling units.
- A second system would cover the area under the access floor in the computer room, entrance facilities, electrical rooms and mechanical rooms.
- A third system is also recommended for the operations centre and printer room, to provide a consistent level of detection for these areas.

UK

BS 5839-1 will be of particular value to the CDCD in determining the requirements for fire safety within the UK.

- BS 5839-1: Fire detection and fire alarm systems for buildings. Code of practice for system design, installation, commissioning and maintenance.

Other Standards cover specific areas or components of the facility.

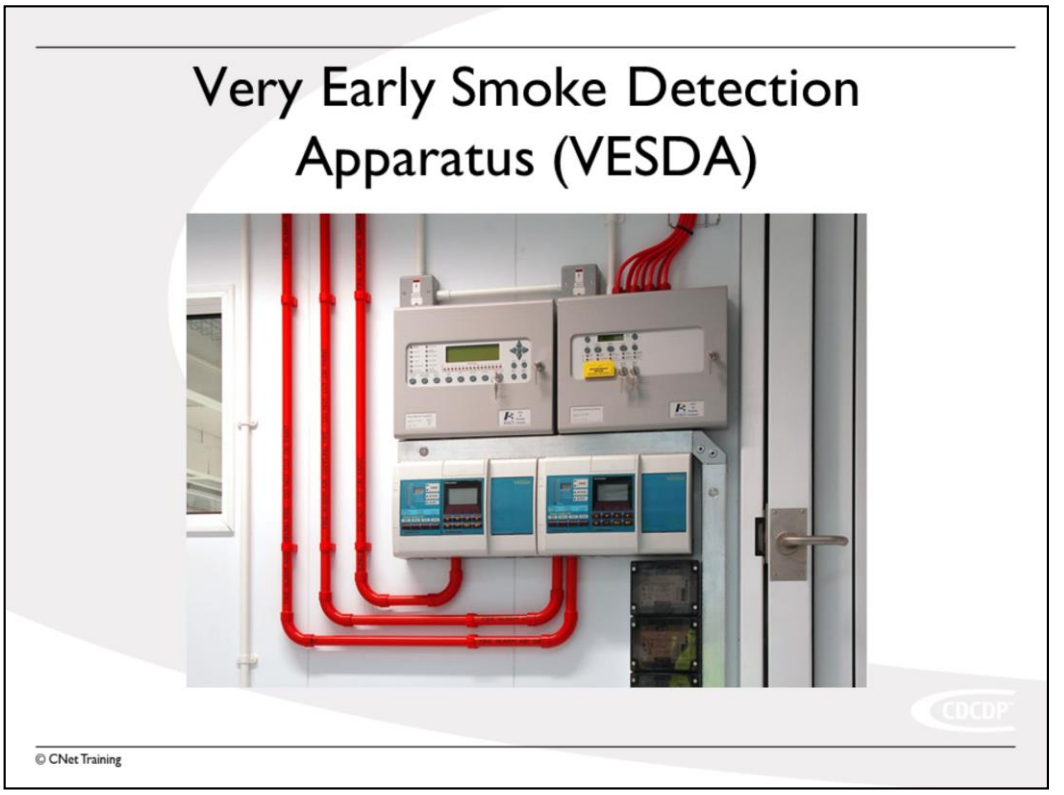
- BS EN 54: Covering general requirements of fire alarm and detection components.
- BS 6266: Code of practice for fire protection for computer rooms and other electronic installations.
- BS 8492: Telecommunications equipment and telecommunications cabling – Code of practice for fire performance and protection.

Aspirating Smoke Detection (ASD) is Recommended for Data Centres

- BS 6266 – *'A dedicated smoke detection system interfaced with the main building system, and an aspirating smoke detection to monitor return air flows, for critical equipment areas such as centralised computer facilities.'*
- TIA 942-A
  - The recommended smoke detection system for critical Data Centres containing high airflow will provide early warning via continuous air sampling and particle counting, and have an equal range to that of conventional smoke detectors.
  - Level 3 and 4 Data Centres should have ASD systems.

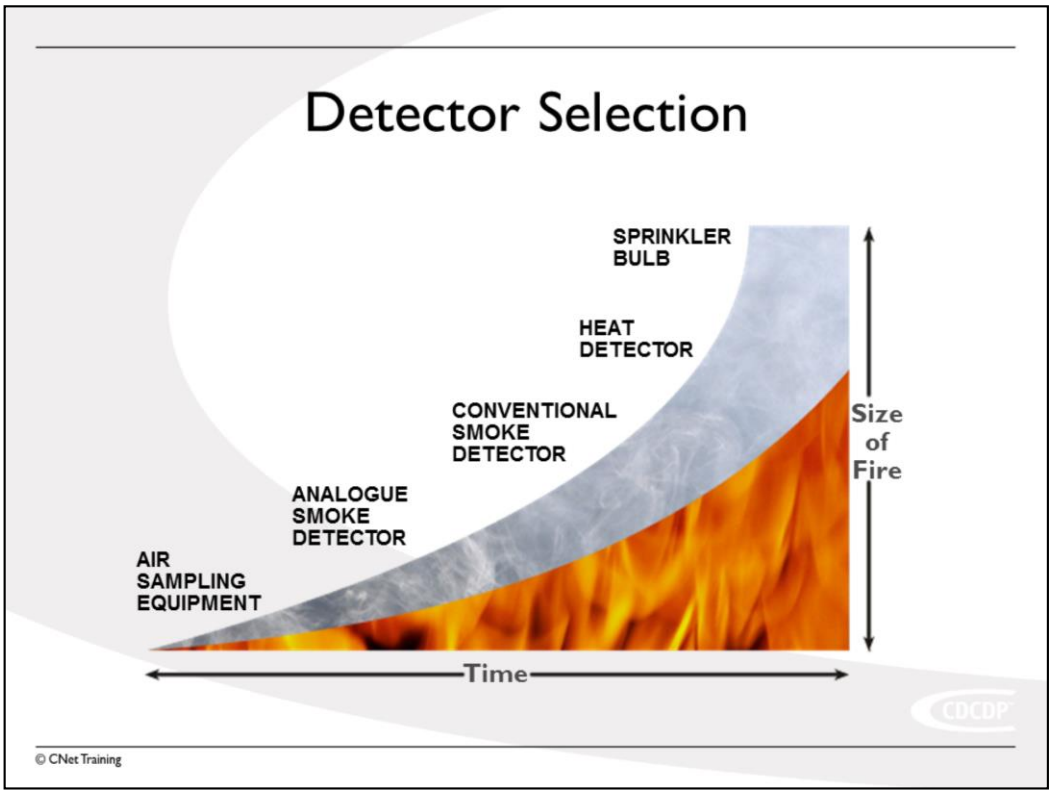
© CNet Training

Aspirating Smoke Detection (ASD) is a high-sensitivity, laser-based optical smoke detection system that continually draws air (within the protected area) through a network of pipes, where it is passed through a calibrated detection chamber. It is capable of providing very early warning of fire conditions, thereby providing invaluable time to investigate and respond to a potential threat of fire.

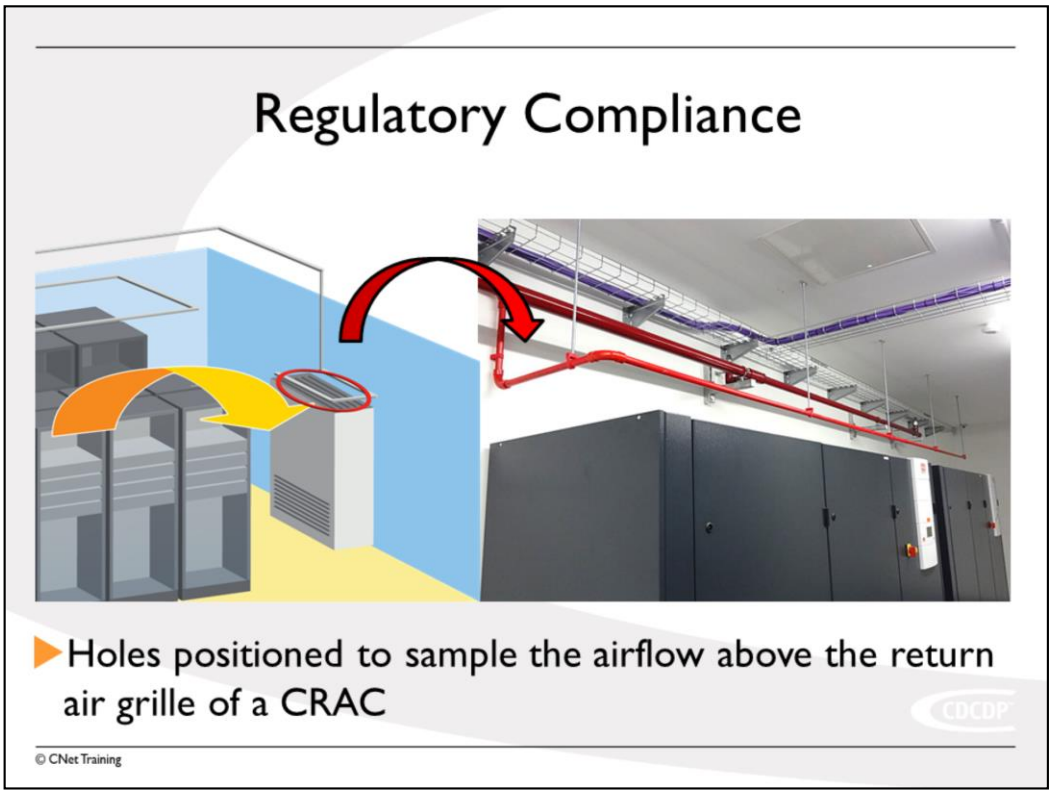


VESDA is a well-respected system often found in Data Centres. VESDA works by continuously drawing air into a distributed pipe network via a high-efficiency aspirator. The air sample then passes through a dual-stage filter. The first stage removes dust and dirt from the air sample before it enters the laser detection chamber.

The second, ultra-fine stage provides an additional clean-air supply to keep the detector's optical surfaces free from contamination, ensuring stable calibration and long detector life, as well as minimising nuisance alarms. From the filter, the air sample goes through the calibrated detection chamber, where it is exposed to a laser light source. When smoke is present, light is scattered within the detection chamber and is instantly identified by the highly-sensitive receiver system. The signal is then processed and presented via a bar-graph display, alarm threshold indicators and/or graphic display. VESDA detectors are able to communicate this information to a fire alarm control panel, a software management system, or a Building Management System (BMS) via relays, or a High Level Interface (HLI).

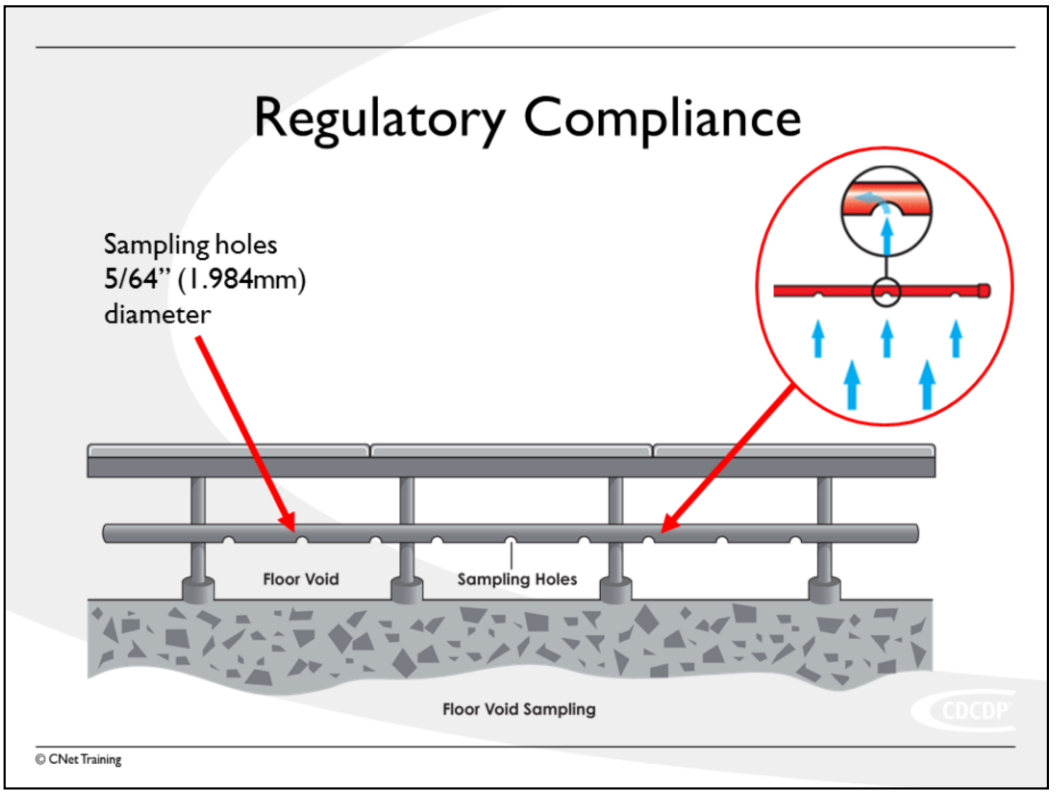


There are different types of detector, each having its own reaction time. The choice is therefore based on the findings of the risk assessment.

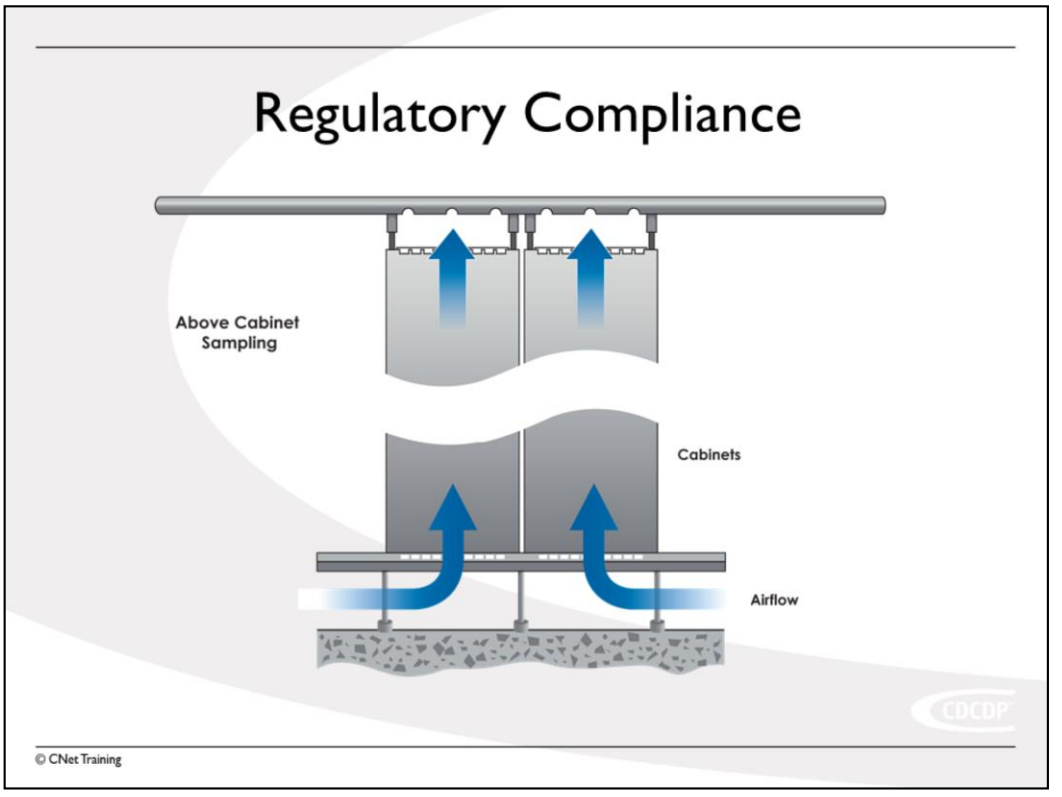


Air sampling provides a compliant design. Installing sampling points where conventional detectors would have been placed in the ceiling is the recommended practice.

Smoke in an air conditioned room travels with the airflow to the return air grille of the CRAC. Sample holes placed at the grille afford optimum protection, and some Standards recommend 1m separation.



The sampling holes point down to detect rising smoke, and to avoid dust dropping from the underside of the raised floor, causing false operation.



Sampling points above cabinets are also a good idea. In practice, this means they are located down the centre of the hot aisle in a Data Centre.

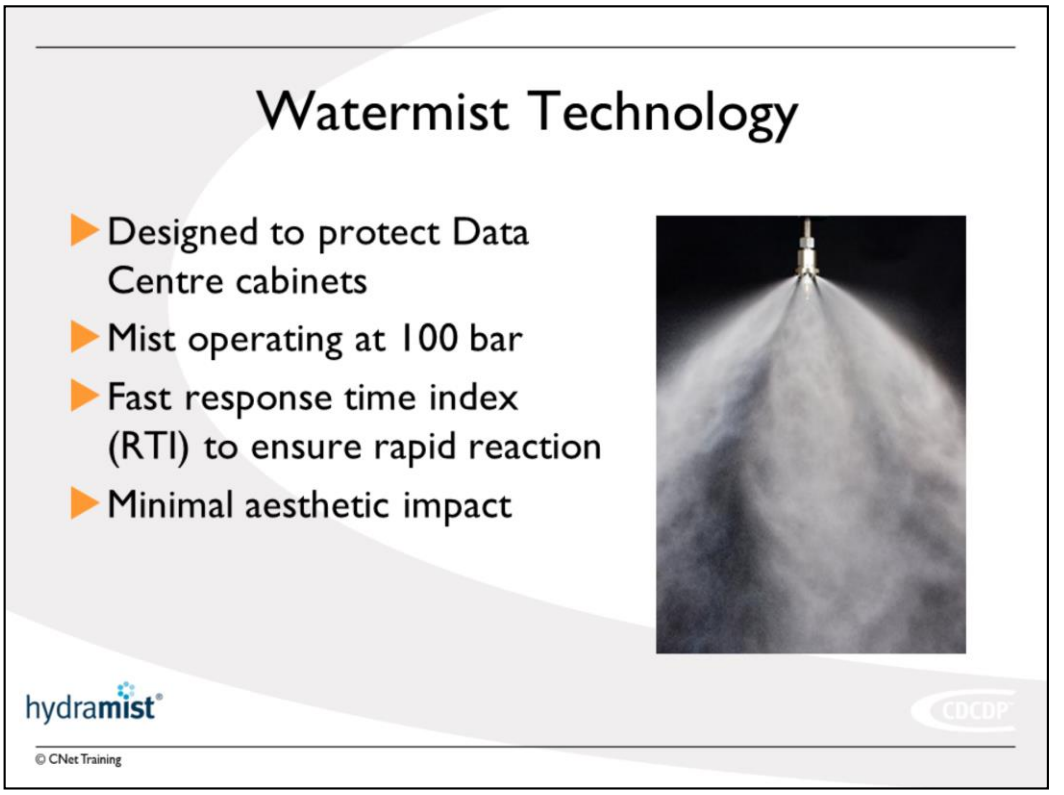
However, in general, such protection should be avoided whenever possible, as its effectiveness is usually limited to certain applications where the floor is over 410mm (16in) high, and the combustible loading under the floor is significant.

Where the need for a suppression system in a subfloor space is deemed appropriate, consideration should also be given to clean agent systems as an alternate.

A pre-action sprinkler system contains no water in the sprinkler piping or at the sprinkler heads under normal conditions.

It is often referred to as a closed system, and is used to provide fire suppression in water-sensitive environments where serious water damage occurs from a broken sprinkler head or the piping.

A pre-action sprinkler system provides the next level of protection for the Data Centre as it affords a higher level of reliability and risk mitigation. The pre-action system is normally air-filled, and will only allow water in the piping above the Data Centre when the smoke detection system indicates there is an event in progress. Once the water is released into the piping, it still requires a sprinkler to activate before water is released into the room.



Watermist technology is designed as a local application solution to protect each Data Centre cabinet. The high pressure Watermist system is very effective at extinguishing fire, with specially designed pumps and engineered nozzles creating a fine mist, operating around 100 bar. The mist presents no risk to either personnel or the environment, and is ideal for the Data Centre.

There are a range of nozzles, designed to produce high pressure water mist with enough flow and velocity to effectively suppress and extinguish fires in a wide range of applications. Fast Response Time Index (RTI) properties incorporated in the nozzle design ensure rapid reaction to fire and maximise the effectiveness of the system. Minimal aesthetic impact is achieved by the low profile dimensions of the nozzle range.

Gaseous Fire Suppression: Clean Agent Systems

- High level of protection
- Installed in addition to:
  - Pre-action sprinkler
  - Smoke detection
- Fully floods room and underfloor areas

© CNet Training

A clean agent fire suppression system provides the highest level of protection for the computer room and associated electrical and mechanical rooms.

This system can be installed in addition to the pre-action suppression and smoke detection systems. The fire suppression system is designed (upon activation) to have the clean agent gas fully flood the room and the subfloor areas.

Effective room sealing is required to contain the clean agent, so effective concentrations are achieved and maintained long enough to extinguish the fire.

NFPA recommends electronic and HVAC equipment be automatically shut down in the event of any suppression system discharge.

Clean Agent Fire Suppression System: INERGEN

- INERGEN® is a mixture of nitrogen, argon and carbon dioxide, and extinguishes fire by reducing the oxygen level in the area to below 15%, the point at which most combustibles will no longer burn

ANSUL

© CNet Training

The INERGEN fire suppression system protects enclosed areas where people may be present. Upon discharge, INERGEN agent fills the room, mixing with the air to suppress fires quickly and effectively. Safe for people, INERGEN agent is non-synthetic and made of naturally-occurring gases - nitrogen (52%), argon (40%) and carbon dioxide (8%). Once discharged, it returns to the atmosphere in its natural state. INERGEN agent is free of residues and corrosive by-products that may produce further property damage. Subsequently, it poses no ozone-depleting or global warming threat.

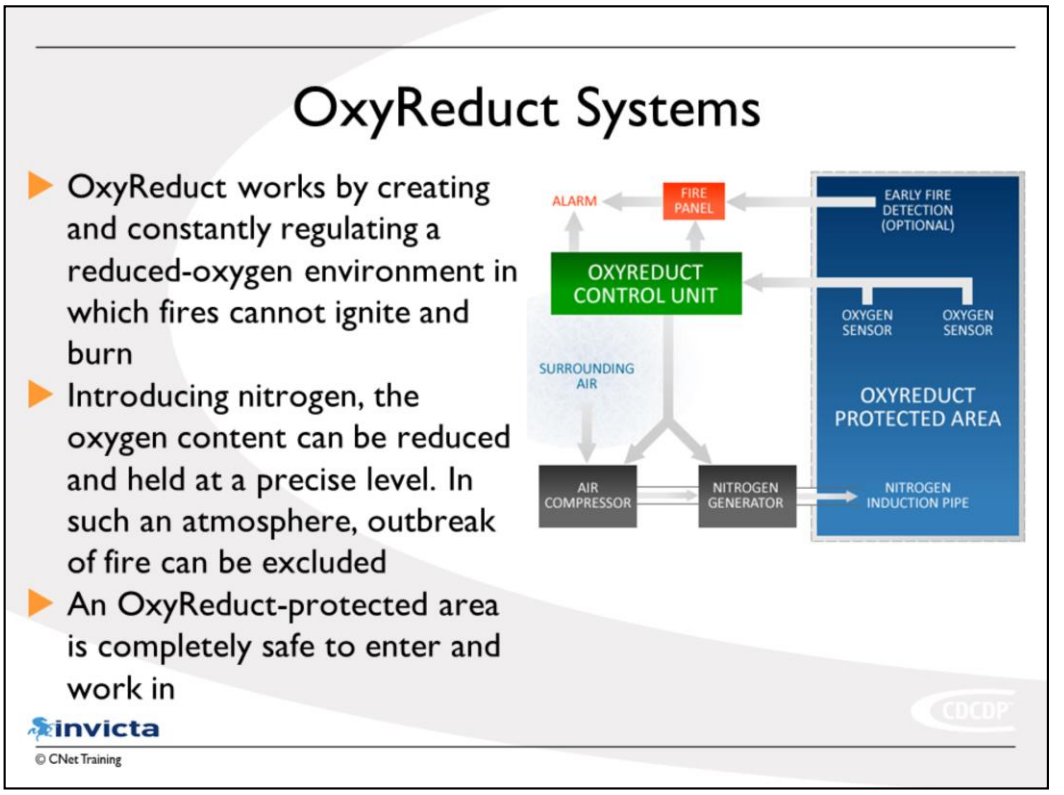
Clean Agent Fire Suppression System: FM200

- FM200 is chemically known as Heptafluoropropane, sometimes referred to as HFC-227ea. It is a colourless, liquefied, compressed gas. It is stored as a liquid and dispensed into the hazard as an electrically non-conductive vapour.
- FM200 extinguishes fire by both its chemical effect (80%) and its physical effect (20%). It has been classified suitable for use as a total flooding agent in occupied areas.

© CNet Training

FM-200 is stored as a liquid in pressurised cylinders at 25/42/50 bar at 21° C. In the event of a fire, the system fire alarm signals the condition, activating the electromagnetic actuator, which opens the valve on the cylinder containing FM-200 gas. When the system is activated, FM-200 gas evaporates at the spray nozzles and suppresses the fire in the form of gas.

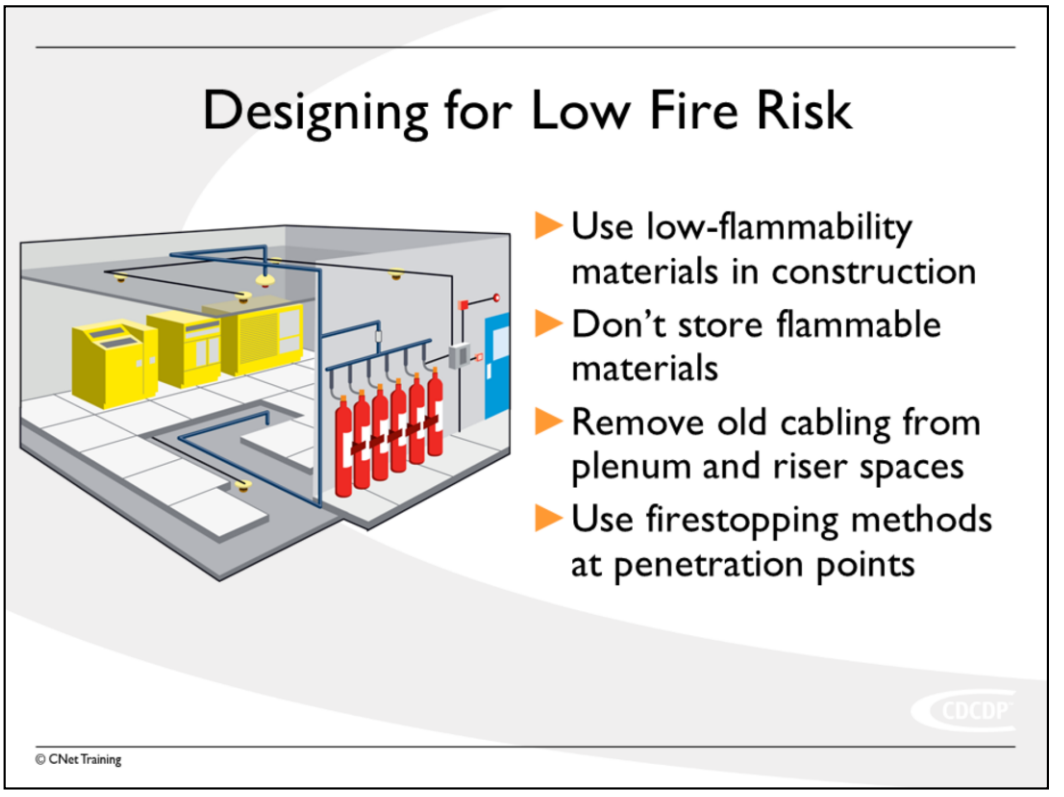
Due to decomposition of the gas at high temperatures developing in a fire, the discharge time of the gas is a maximum of 10 seconds at 20° C. During discharge in the protected zone, first a negative pressure occurs (due to a slight cooling of the room), followed by overpressure. In order to ensure the integrity of the protected zone, it is essential to ensure pressure compensation (i.e., to secure the protected zone from damage, which could occur in the fire extinguishing process).



OxyReduct works by creating and constantly regulating a reduced-oxygen environment within which fires cannot ignite and burn. The system operates 24x7x365, constantly monitoring oxygen levels within the controlled environment, making adjustments accordingly, requiring no manual intervention.

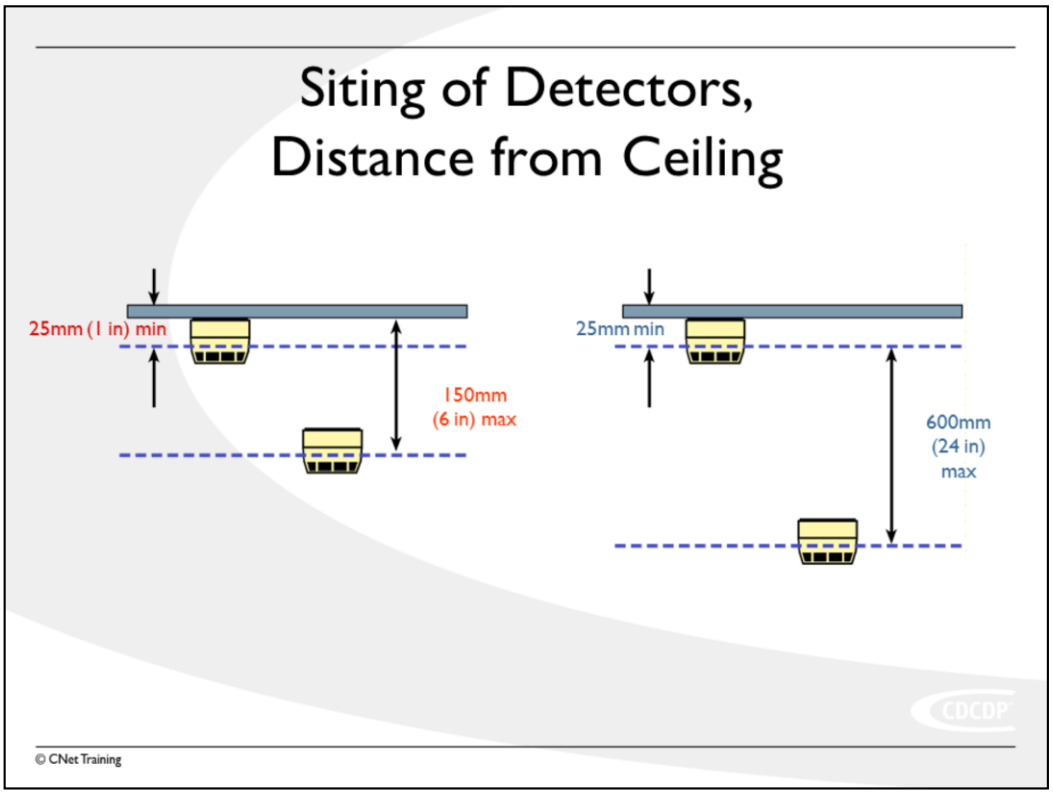
As OxyReduct is not a reactive system, like traditional gas suppression and sprinkler systems which only activate once a fire has actually started; there is no resulting damage to any items contained within the area, and no electrical power downtime whilst the source of the fire is investigated.

It has a self-checking system technology (constant monitoring of room density, unit function and effectiveness, and logging).

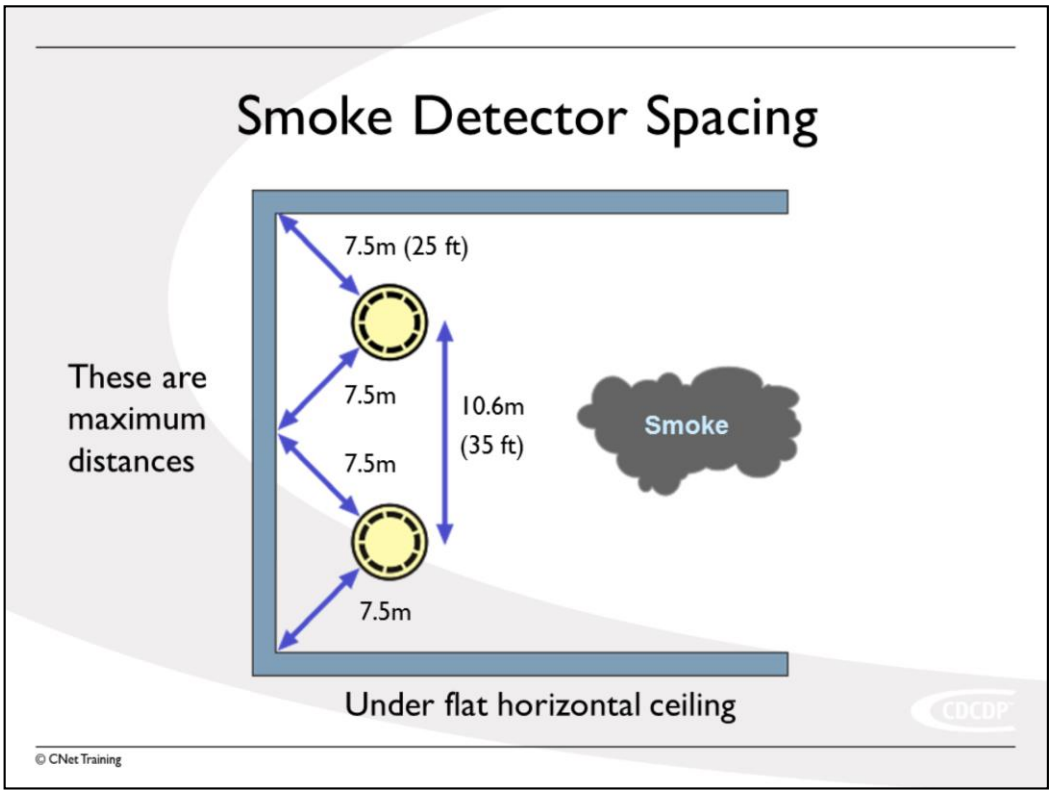


The basic consideration is to reduce the potential fuel load in the space, followed by containing any consequences.

- Don't store flammable materials in the computer room - for example, storage tapes could be kept in a separate room.
- Remove old cable. In the US, it is a legal requirement under the NEC that abandoned cables are removed.

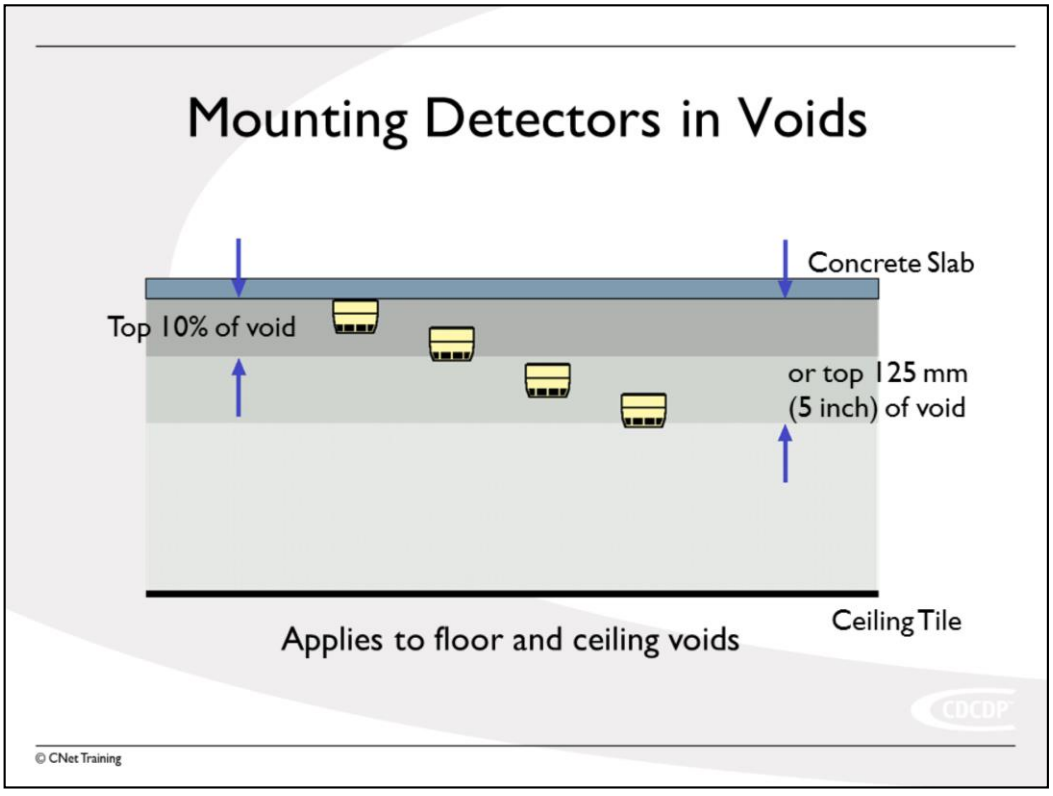


Guidelines are available which specify where the smoke and / or heat detectors should be placed to ensure correct operation. As a CDCD, you should also check local regulations that may be defined by the Authority Having Jurisdiction (AHJ).

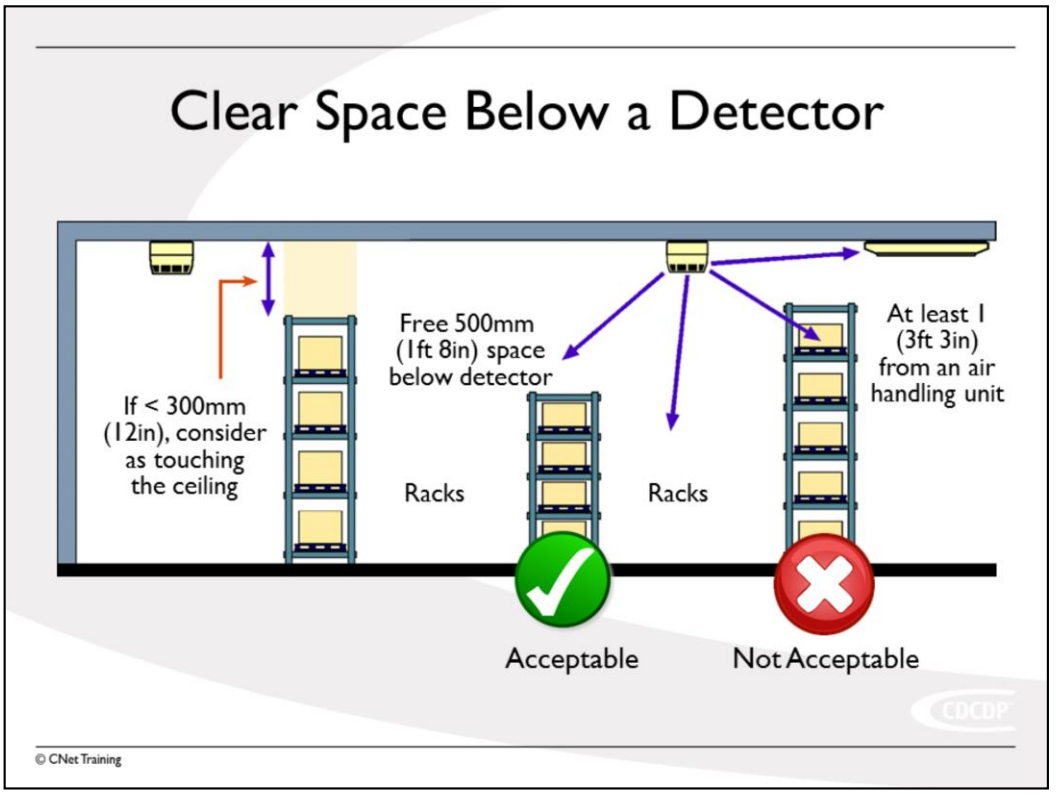


Maximum distances are detailed above. Lateral spacing is also a major consideration. For corridors, the final detector shall be 5.3m (17ft 5in) from the end wall, and 10.6m (35ft) thereafter.

If it is too close to the corner, smoke will swirl and miss the detector.

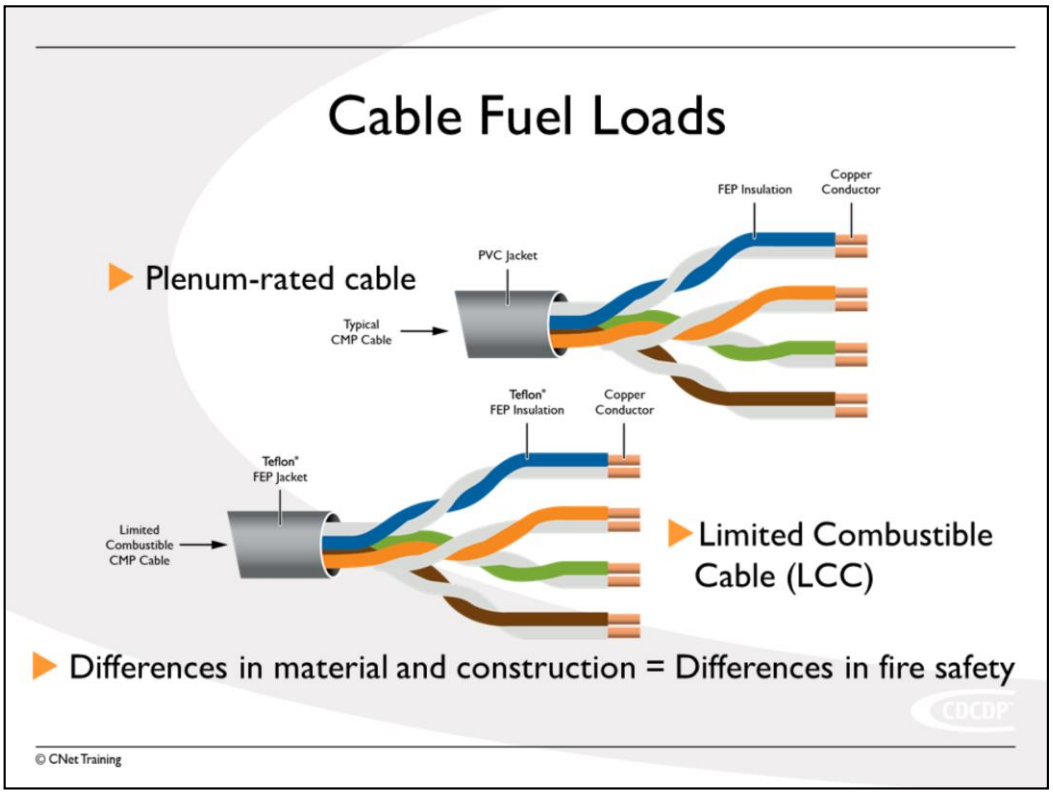


Floor and ceiling voids should be included in the detector location plans.

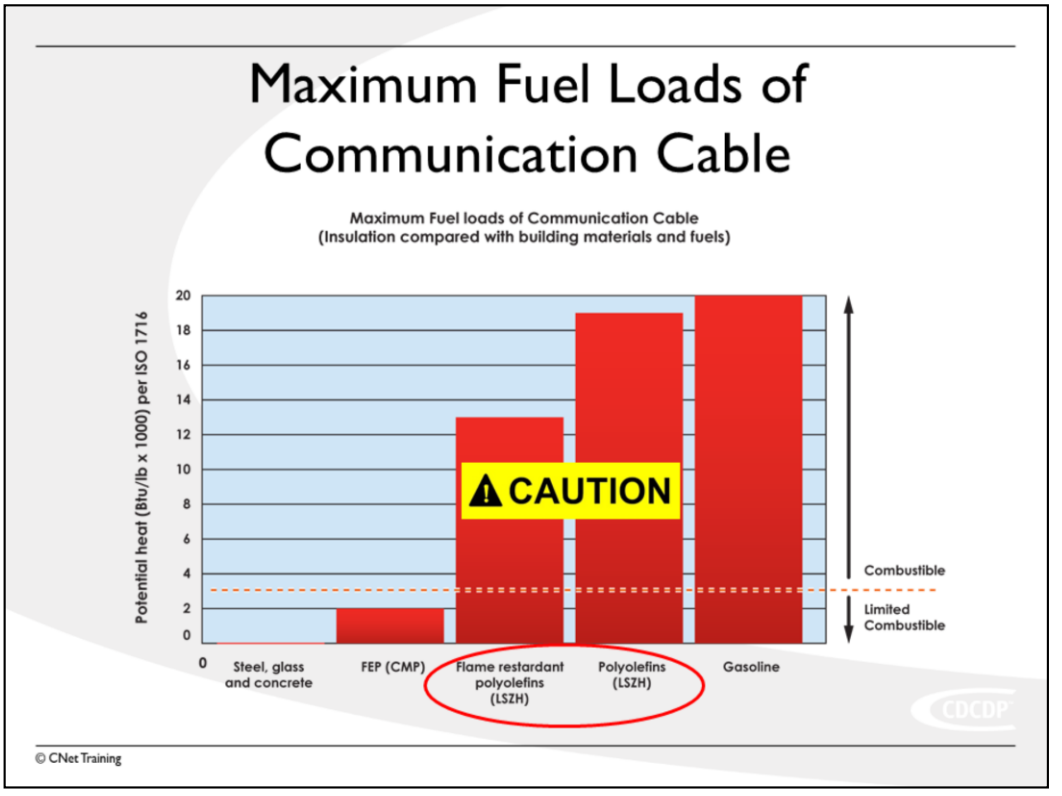


Cabinets that have less than 300mm (12in) of clear space above them should be regarded as touching the ceiling. A detector is therefore required on each side.

There should be adequate space below the detector to allow airflow to carry any smoke to it. Too close to an air handling unit and the smoke may miss the detector altogether.

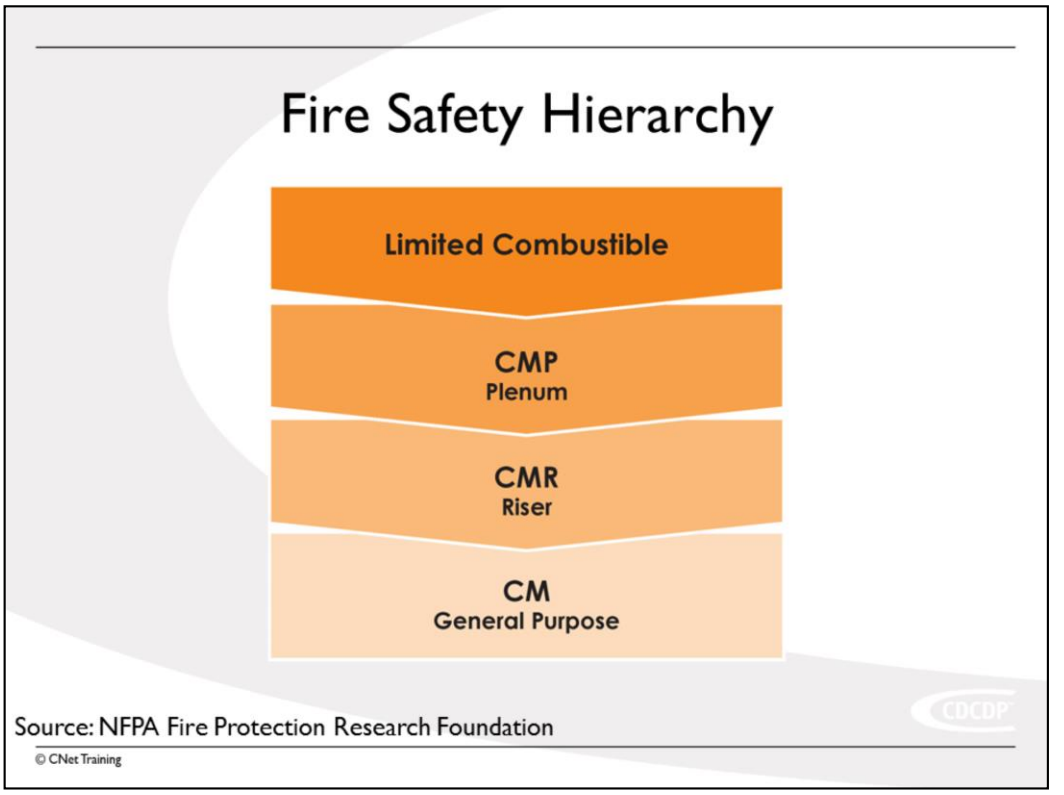


Materials really do make a difference to the fire performance. Limited Combustible Cable (LCC), also called CMP-50 cable, is fire-resistant, with insulation made of a synthetic material called Fluorinated Ethylene Propylene (FEP). This insulation allows LCC to withstand higher temperatures for longer periods of time than ordinary cable. Another advantage of LCC is that it lasts longer before the insulation begins to contaminate the cable - a process that is an inevitable part of cable aging that can increase cable loss. In addition, LCC is more tolerant of prolonged high humidity or exposure to corrosive chemicals or pollutants.



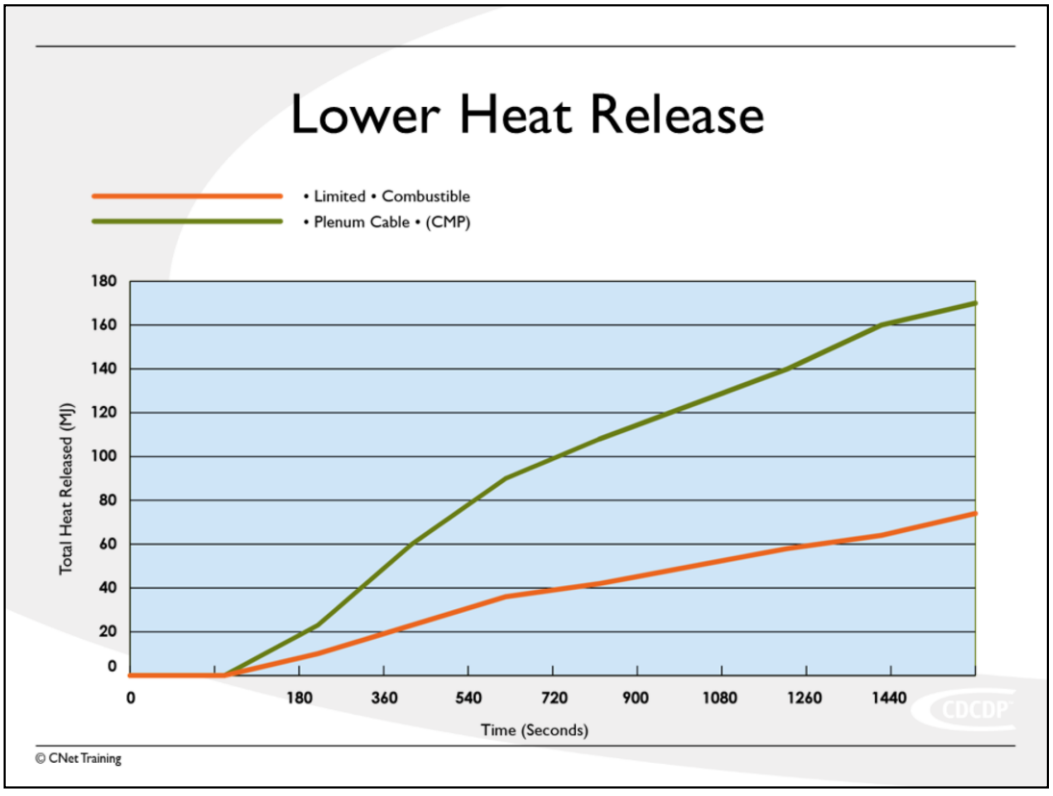
In the US, limited combustible cables are used in risers and voids, as they smoulder rather than burn. They do, however, give off poisonous fumes.

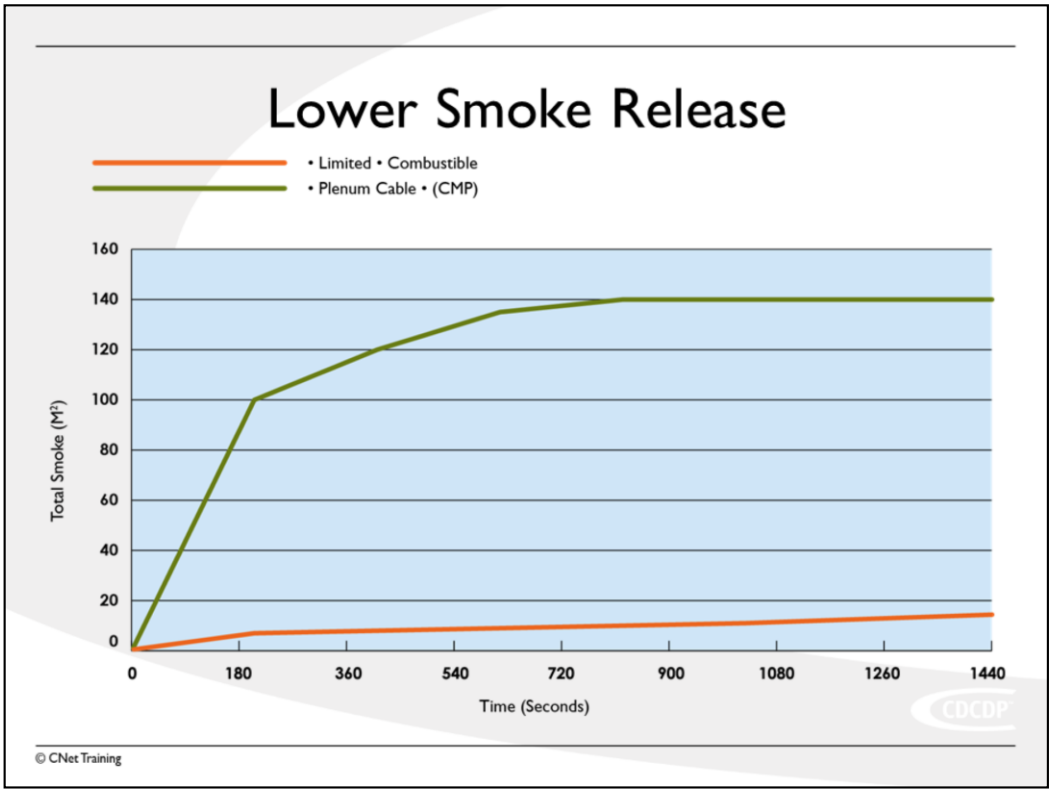
In Europe, LSZH cables are used since they do not give off poisonous fumes. LSZH burns very well, as shown in the graph above.

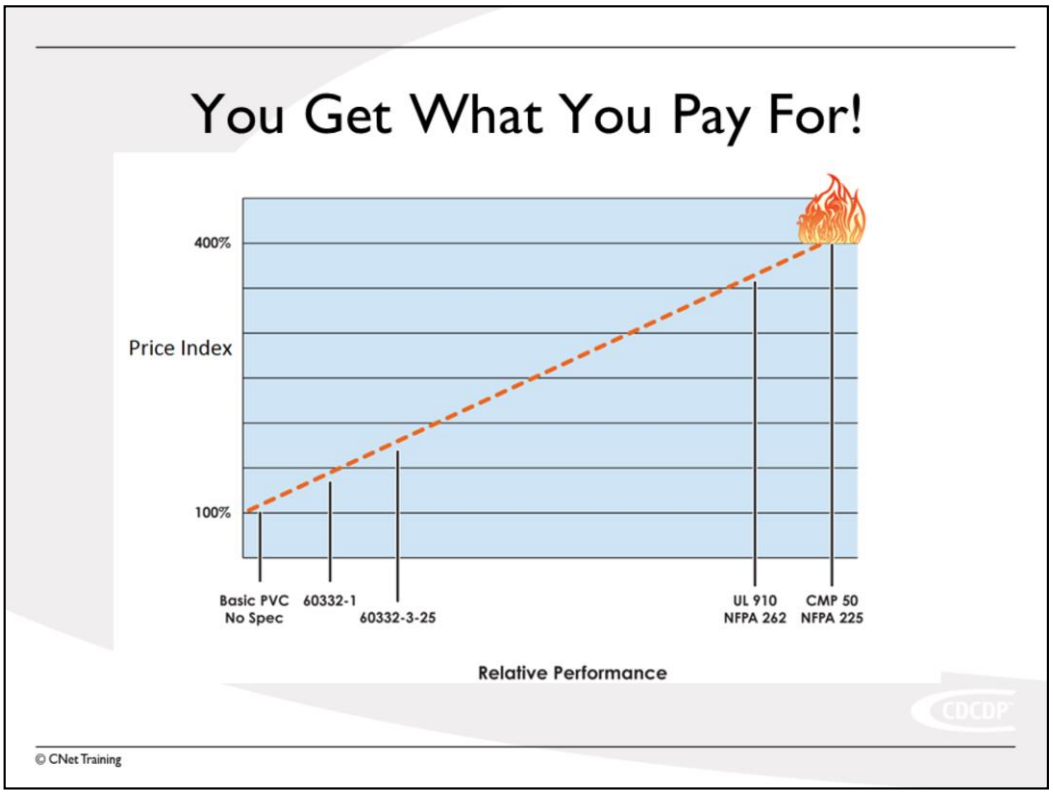


US building codes are quite specific in which cable type to use for a given situation. Limited combustible cables reduce smoke up to 20 times more than conventional plenum cables, reducing the risk of damage to sensitive electronic equipment, such as those found in networks and Data Centres. Limited combustible cables also offer greater environmental sustainability than typical combustible wire and cable products due to the following:

- Do not contain any substances or components regulated under the RoHS (Restriction of Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment) Directive
- Free of heavy metals and phthalates (Phthalates are a group of chemicals used to make plastics more flexible and harder to break)
- Offer more complete recyclability of both copper and plastics at end-of-life
- Contain post-industrial recycled content today, with options for post-consumer content in the future (Source: DuPont)


Lower Heat Release
• Limited • Combustible
• Plenum Cable • (CMP)
Total Heat Released (MJ)
180
160
140
120
100
80
60
40
20
0
0
180
360
540
720
900
1080
1260
1440
Time (Seconds)
CDCDP
© CNet Training

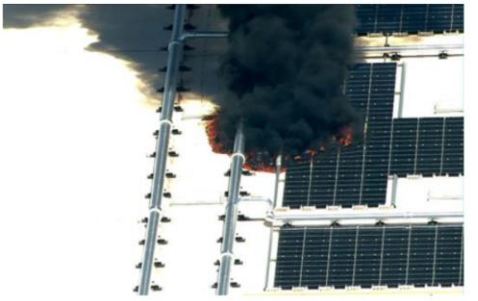

Lower Smoke Release
• Limited • Combustible
• Plenum Cable • (CMP)
Total Smoke (M²)
160
140
120
100
80
60
40
20
0
0
180
360
540
720
900
1080
1260
1440
Time (Seconds)
CDCDP
© CNet Training



The better the fire performance of the cabling, the higher the cost. Very often, budget dictates which type is specified. That said, the local codes or regulations may be the deciding factor - check with the AHJ.

Fire Risk to a Data Centre

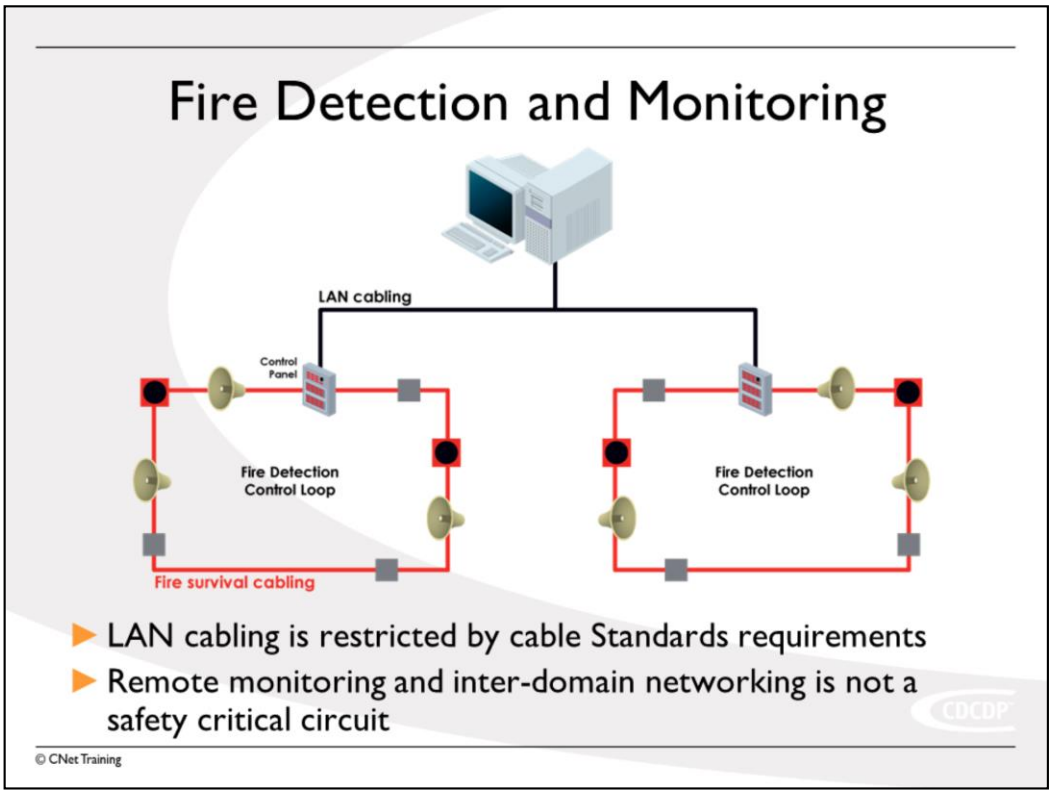
Samsung Data Centre
South Korea



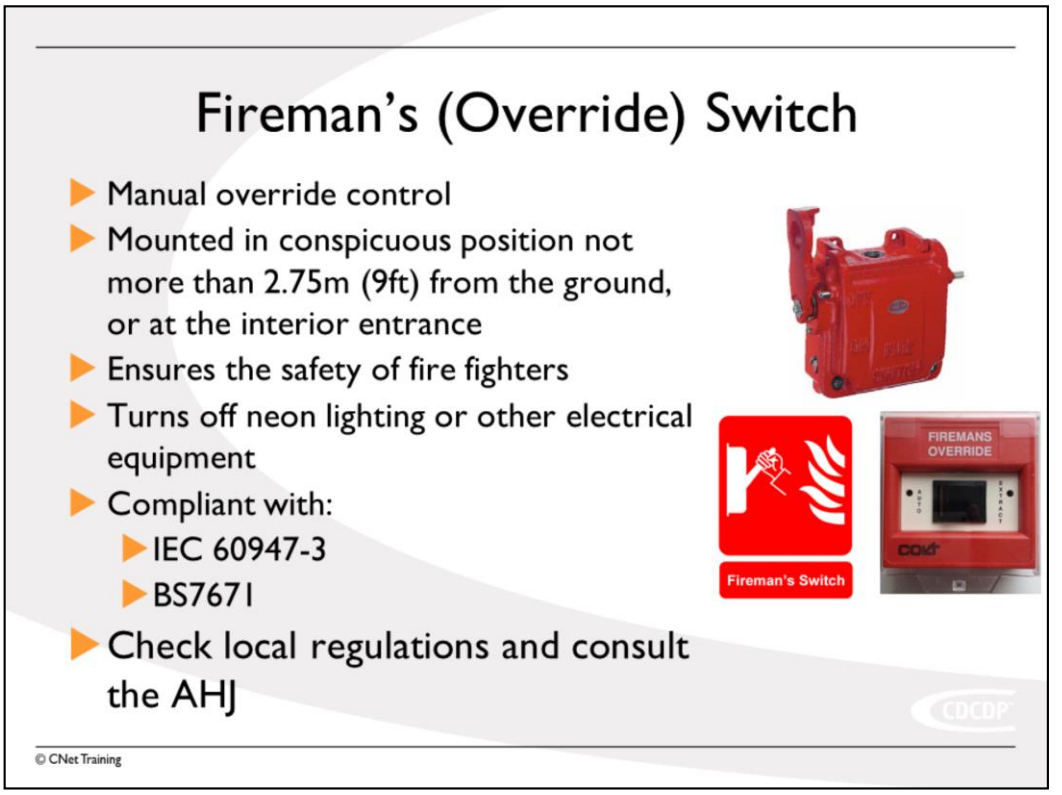
Apple Data Centre
Mesa, Arizona

- A genuine risk that needs to be properly evaluated

© CNet Training



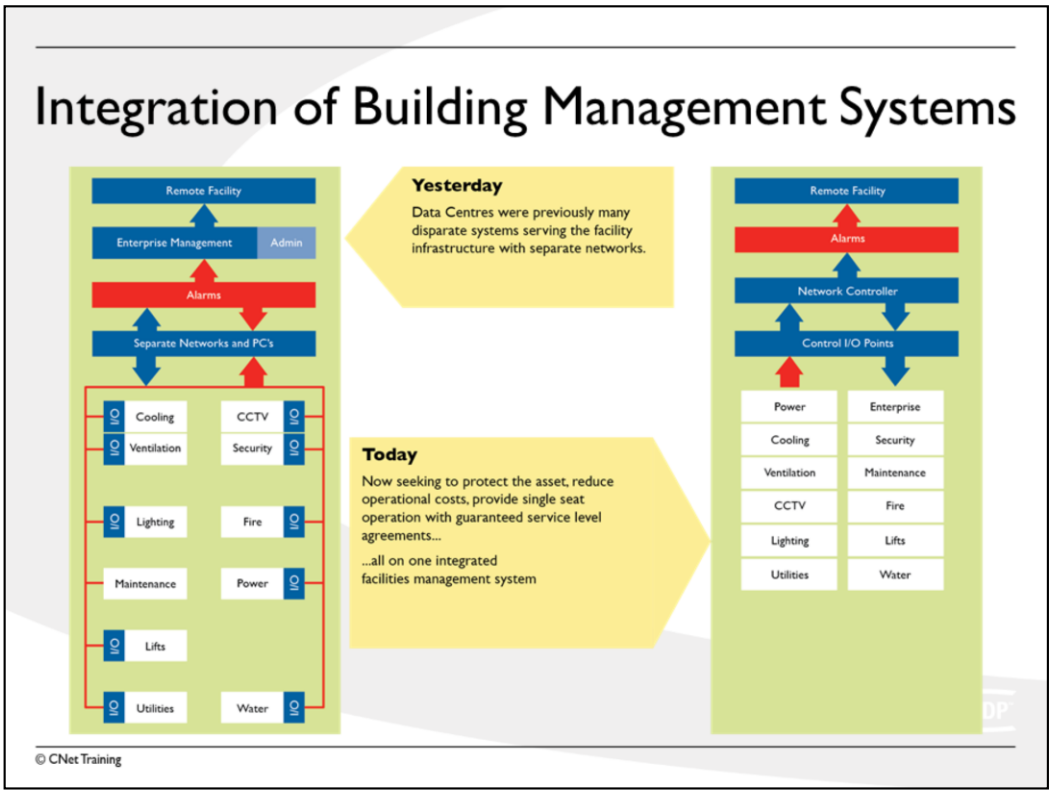
As mentioned previously, the fire control loop, as shown above, will need to be connected with fire survival cabling, whereas the supervisor and inter-domain connection can utilise normal network cabling, e.g., Cat 5e.



The fireman switch is a specialised switch disconnect / isolator. They are used by firemen to turn off neon-lighting or other electrical equipment in case of fire, to prevent overheated equipment from exploding.

Where any circuit operates at a potential difference exceeding low voltage, a fireman's emergency switch must be provided. Such installations usually take the form of discharge lighting (neon signs); this requirement applies to all external systems, as well as internal signs which operate unattended. The purpose is to ensure the safety of fire fighters who may (if a higher-voltage system is still energised) receive dangerous shocks when they place a water jet on. The fireman's switch must meet the following requirements:

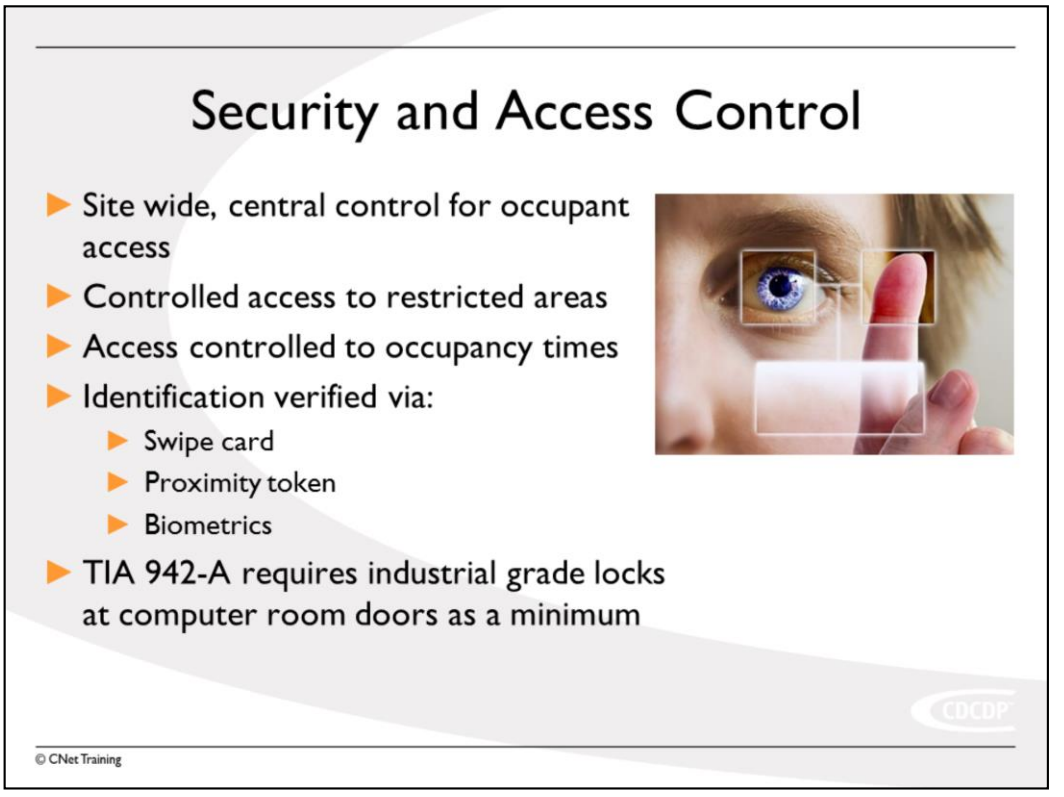
- The switch must be mounted in a conspicuous position not more than 2.75m (9ft) from the ground.
- It must be coloured red and have a label in lettering at least 13mm (0.51in) high - 'FIREMAN'S SWITCH'. On and off positions should be clearly marked, and the OFF position should be at the top. A lock or catch should be provided to prevent accidental reclosure.
- For exterior installations, the switch should be close to the load, or to a notice that clearly indicates the position of the well-identified device.
- For interior installations, the switch should be at the main entrance to the building.
- Ideally, no more than one internal and one external switch must be provided. Where more become necessary, each switch must be clearly marked to indicate *exactly* which parts of the installation it controls.
- Where the local fire authority has additional requirements, these must be followed.
- The switch should be arranged on the supply side of the step-up sign transformer.



A Building Management System (BMS) is used to provide an optimised system of control and monitoring services for effective building operations. In a Data Centre, systems that are monitored typically include power, heating, ventilation, air conditioning, security and access control.

In all tier levels, it is a mandatory requirement to have monitoring systems in place, with their complexity increasing as the tier level rises. There is a trend towards an all-inclusive BMS system.

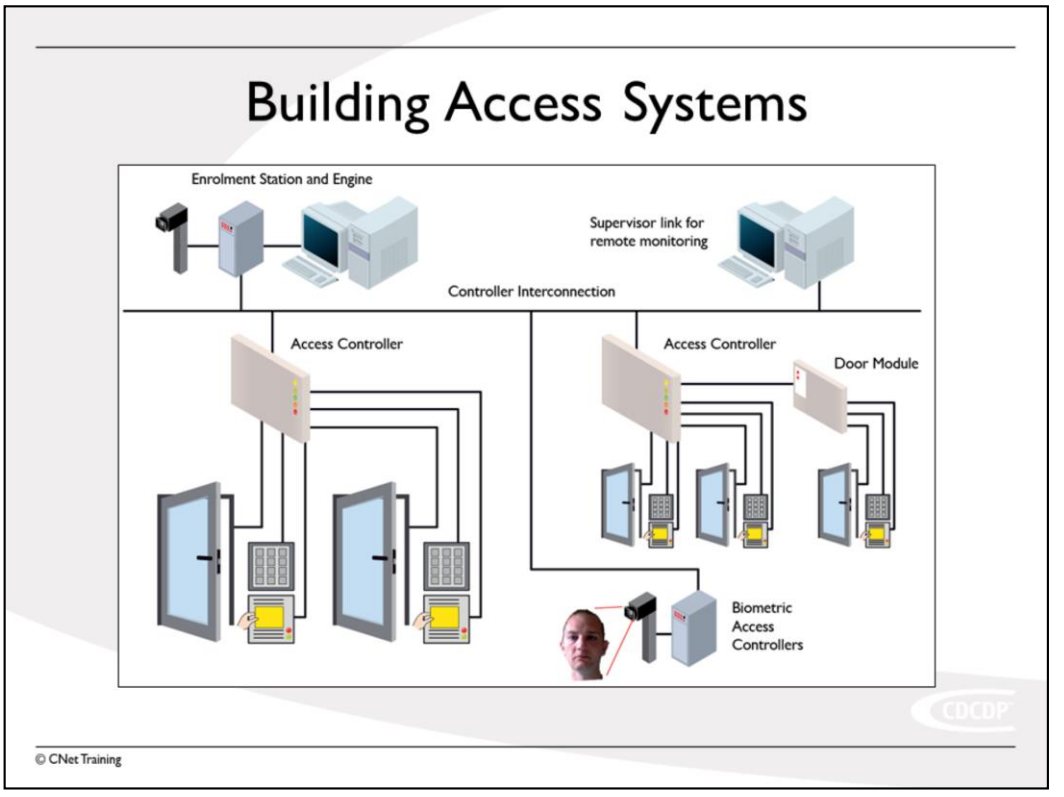
Could it be possible to have all Data Centre environmental monitoring and alarms linked into the BMS? A key question the CDCD must consider.



Security and access control measures are very important in the protection of a facility from unauthorised individuals. Other questions that may need to be answered include:

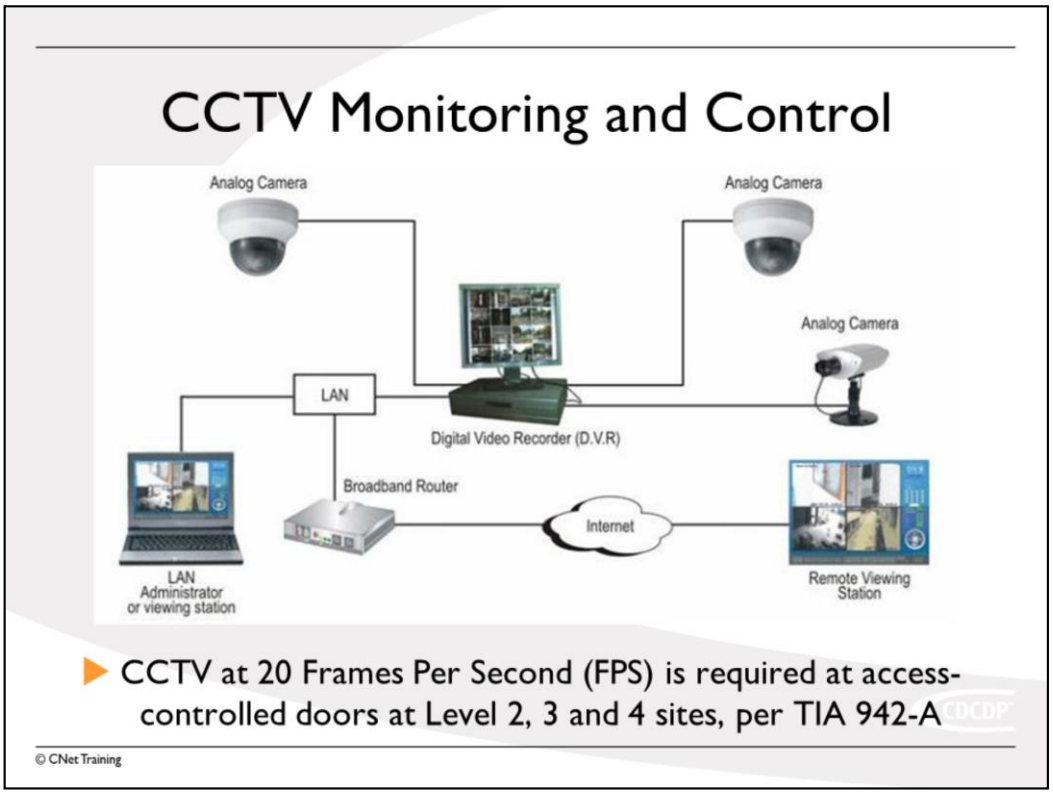
- Can internal doors be locked when left unattended for long periods?
- Are all fire doors alarmed?
- If you have a burglar alarm, are staff familiar with the procedures for switching it on and off?
- Do you maintain good visibility around the perimeter of your building by cutting back overgrown plants, trees and foliage?
- Do you have adequate lighting around your building during the hours of darkness?
- **Access control:** The access system will allow a security or facilities manager to determine access rights to specific areas of the building. Access can be controlled with occupancy times and identification can be done via any of the following:
- **Swipe card:** Traditional credit card-style identification card, programmed into the system. The user must swipe the card through a reader to gain access.
- **Proximity detectors**: An extension of the swipe card - Access is achieved by placing the identification card in the proximity of the sensor, as opposed to swiping through a reader.
- **Biometrics:** Any form of identification using the physiology of an individual; includes such devices as fingerprint scanners, voice, iris and facial recognition.

In higher-security sites, any number of these features may be combined at a single doorway / access point – e.g., Swipe card + Biometric scanner; dual-authentication configurations such as these are becoming more common.



- **Typical Access control system:** The system is a modular structure with distributed intelligence, giving a high degree of autonomy. The system can control a maximum of 999 doors.
- **Controllers:** The controllers can typically control two doors and can be extended to eight doors, using local RS485 bus and door modules. Controllers can communicate with one another using the network.
- **Supervisor:** Supervisory control allows security or maintenance personnel to remotely configure access rights, it also allows fault and alarm annunciation - for example, reader errors and door-forced alarms.
- **Access control facial recognition system:** Adding to the security features of an access system with the use of biometric recognition. The system utilises access and enrollment stations, with system monitoring from a supervisor engine.

Modern systems can be easily integrated into a network environment to include WAN connectivity. Using network cabling infrastructure, access control can be configured and implemented remotely.



CCTV systems must have the following features:

- Archiving of video and audio to a server, with camera control using motion tracking software
- Time zones, allowing quality and sensitivity of recordings to be adjusted throughout the day
- Motion detection alarms which can modify settings
- Live monitoring of system cameras. In Level 2 and above Data Centres, it is a requirement to have real-time equivalent CCTV coverage. In practice, this equates to 20FPS Motion JPEG
- Playback of stored images from network servers and bidirectional audio interaction

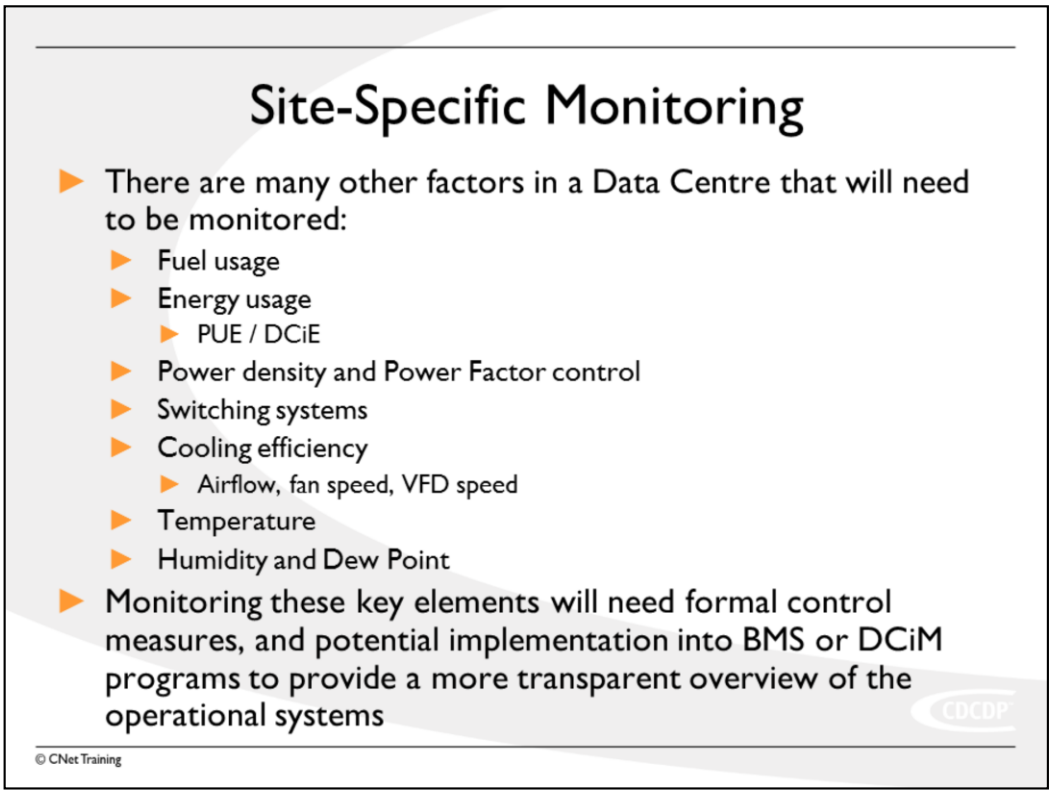
CCTV at 20FPS is required at access-controlled doors at Levels 2, 3 and 4 per TIA 942-A

CCTV Installation and Security Standards

- BS 7958: Closed-circuit television (CCTV) management and operation, code of practice
- BS 8418: Installation and remote monitoring of detector-activated CCTV system, code of practice
- BSEN 50132-5: Alarm systems – CCTV surveillance systems for use in security applications, video transmission
- BS 8495: Code of Practice for the purpose of image export to be used as evidence
- NECA 303: Standard closed-circuit television (CCTV) systems

© CNet Training

CCTV installations must also be cross-referenced against the Data Centre security policy and applicable security Standards.



There are many elements in a Data Centre that will need to be continually measured and monitored to ensure the environments are meeting their respective mission critical capabilities.

The CDCD must therefore bear these in mind when considering applicable design factors. This is likely to involve numerous sensors. Some may be equipment-specific and others environmental; both of which need careful consideration. Implementing effective measuring and monitoring has significant business benefits:

- Provides empirical data to influence recommendations for change
- Provides unambiguous information
- Supports and motivates people by reinforcing recommendations with fact
- Enables better management of the expensive "**4Cs**" - Power, Space, Cooling & Connectivity
- Avoids nugatory Capital Expenditure
- Assists in meeting legislative requirements

Review

- Can you?
  - Design for safety
  - Design for manageability
  - Ensure accurate information sets
  - Implement systems that can be handed over with the Data Centre

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 8

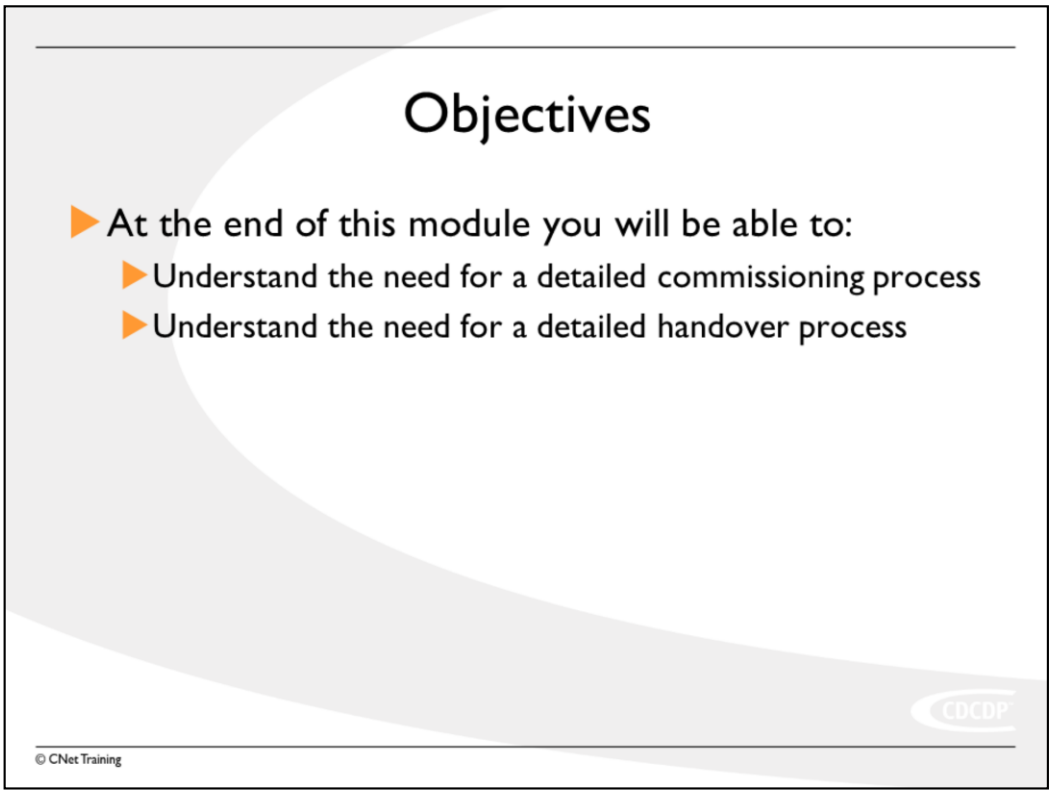
© CNet Training

Certified Data Centre Design (CDCD®) Core Unit

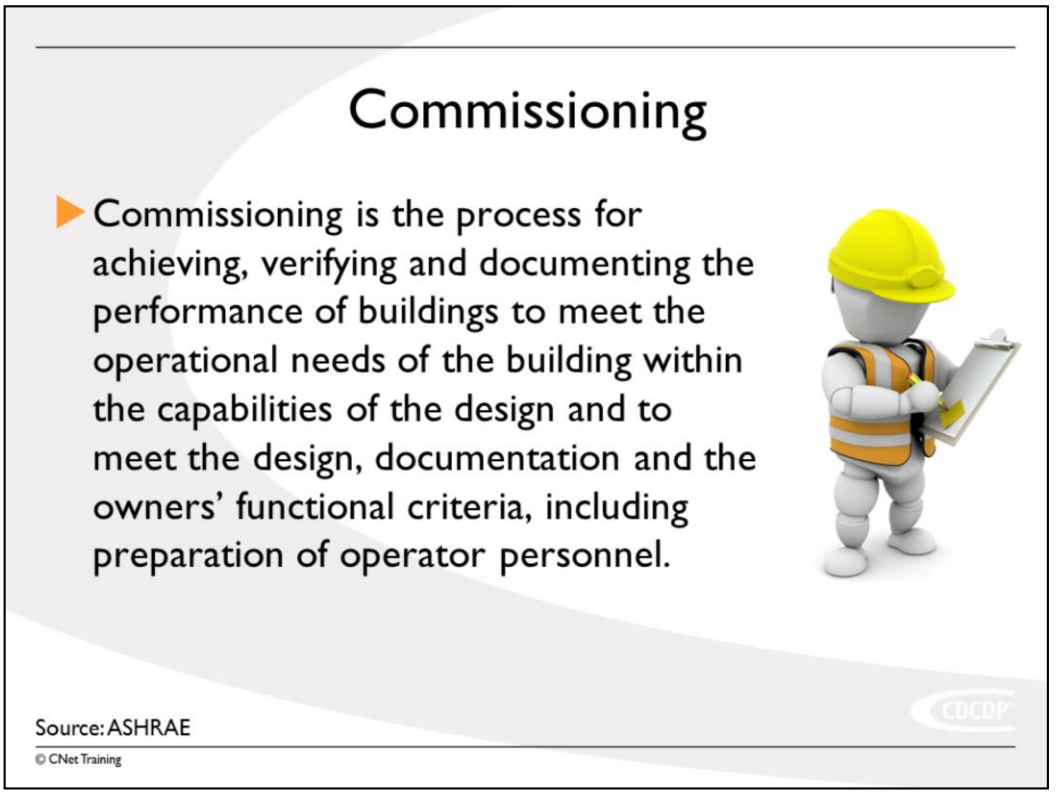
Commissioning and Handover

Version 1509

CDCDP



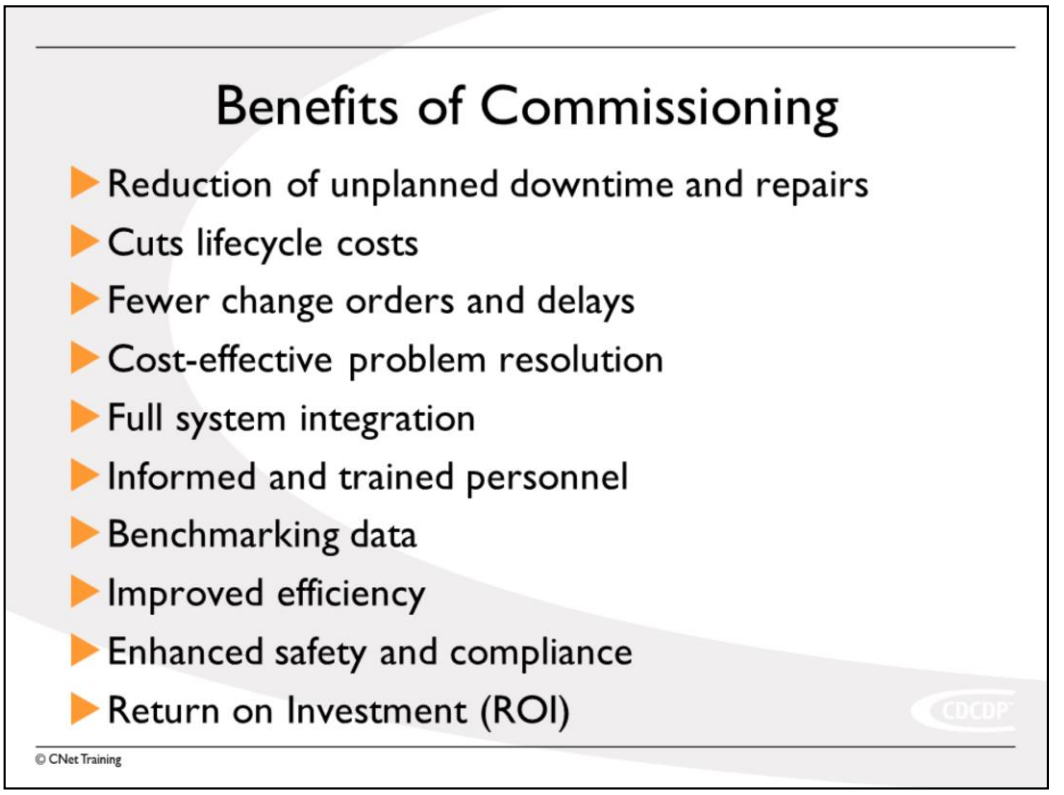
The CDCD must appreciate that the operator has to live with the design for some years, and must consider long-term manageability as a key factor. It is essential the operator fully understands every aspect of the design scope and how it has been implemented.



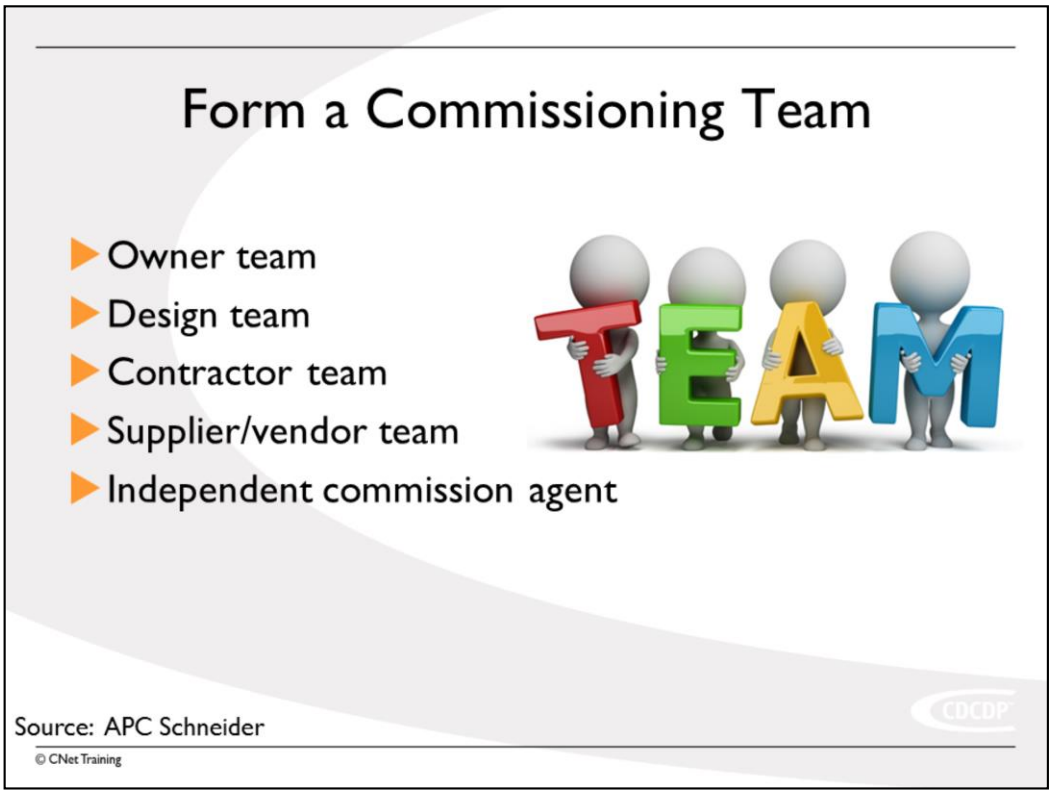
Think right back to the design criteria module, where the need for a project plan for both the design and build was discussed. The handover to the operator is the closing process for this plan.

There will be many commissioning tests required to demonstrate the Data Centre meets the design requirement; these provide the operational basis for the site to maintain or build upon. The tests can be against Standards, manufacturer recommendations, or bespoke requirements from either the CDCD or the customer. Whichever is used, it is necessary to provide evidence of compliance.

A Data Centre will never be 100% compliant on the day it is brought into service. Life does not allow the luxury of waiting until everything is perfect. It will therefore be required to highlight a 'snag list' of variations and actions to be completed after handover, then get the customer to agree to this list!



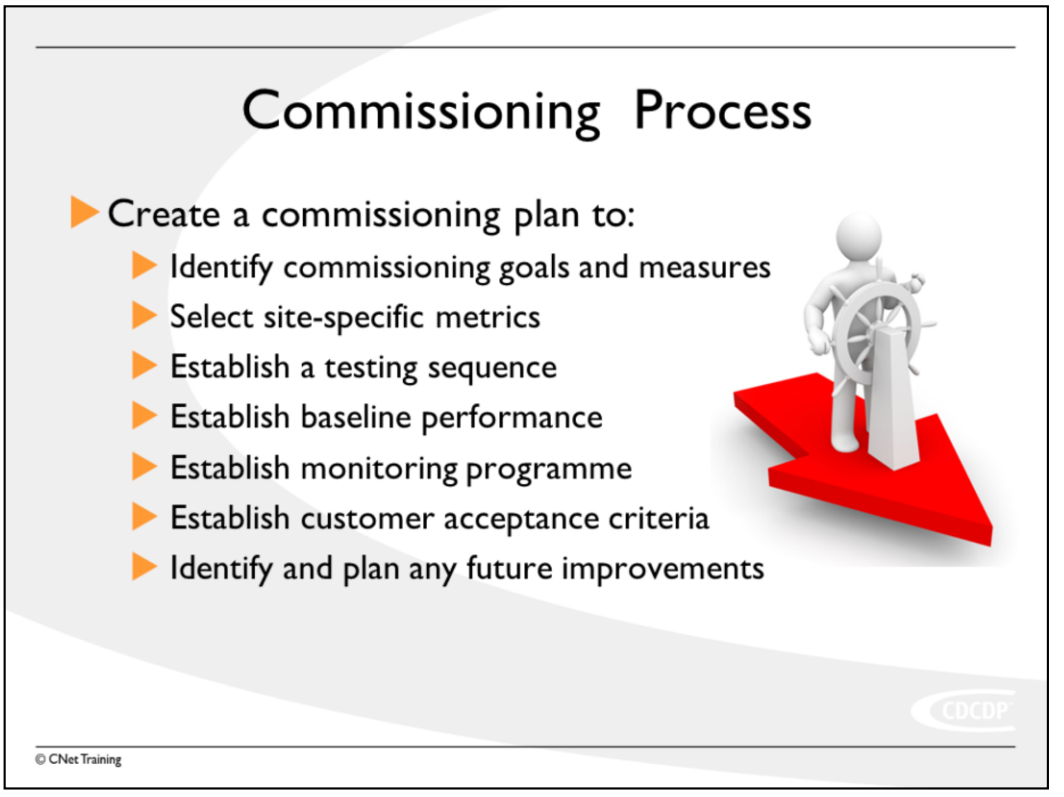
- **Reduced unplanned downtime and fewer repairs** - Preventing or greatly reducing the possibility of unplanned downtime, which can be devastating to a business, is perhaps the greatest value commissioning provides for Data Centre facilities.
- **Reduced lifecycle costs** - Done properly, commissioning improves system performance throughout the lifecycle of a Data Centre. Better system performance not only optimises Data Centre performance, it also decreases operation and maintenance costs, cutting energy consumption for smaller utility bills.
- **Fewer change orders and delays** – Commissioning projects means fewer change orders, delays, and rework, avoiding the considerable costs of late occupancy.
- **Cost-effective problem resolution** - Installation issues are pinpointed before system start-up, and process problems are noted before a component fails.
- **Full system integration** - Complete testing and verification of the functional capability of all system components means they work together as an integrated and functional system.
- **Informed and trained personnel** – Ensures personnel are well-prepared and well-equipped to operate and maintain the newly commissioned system.
- **Benchmarking data** - Commissioning creates extensive documentation for benchmarking system changes and trends. The data can be used to identify future problems with the system or process, maintain optimal operations, and evaluate future maintenance decisions.
- **Improved efficiency** - If efficiency features have been designed and built into the new system, commissioning activities can verify they function as intended.
- **Enhanced safety and compliance** - Reduces owner liability by uncovering safety problems throughout the design, construction, and occupancy phases of a project.
- **Return On Investment** - The benefits of commissioning often create an ROI that far exceeds the cost of the commissioning project itself.



Commissioning teams should consist of the following:

- Owner team, which can include representatives from the IT department, facilities, operations, and key business units
- Design team, which may include an architect / engineer from the outside, an interior designer, and any specialised consultants
- Contractor team, which will include the contractor, external / internal project management, and any significant sub-contractors
- Supplier/vendor team, independent product representatives including separate commissioning agent

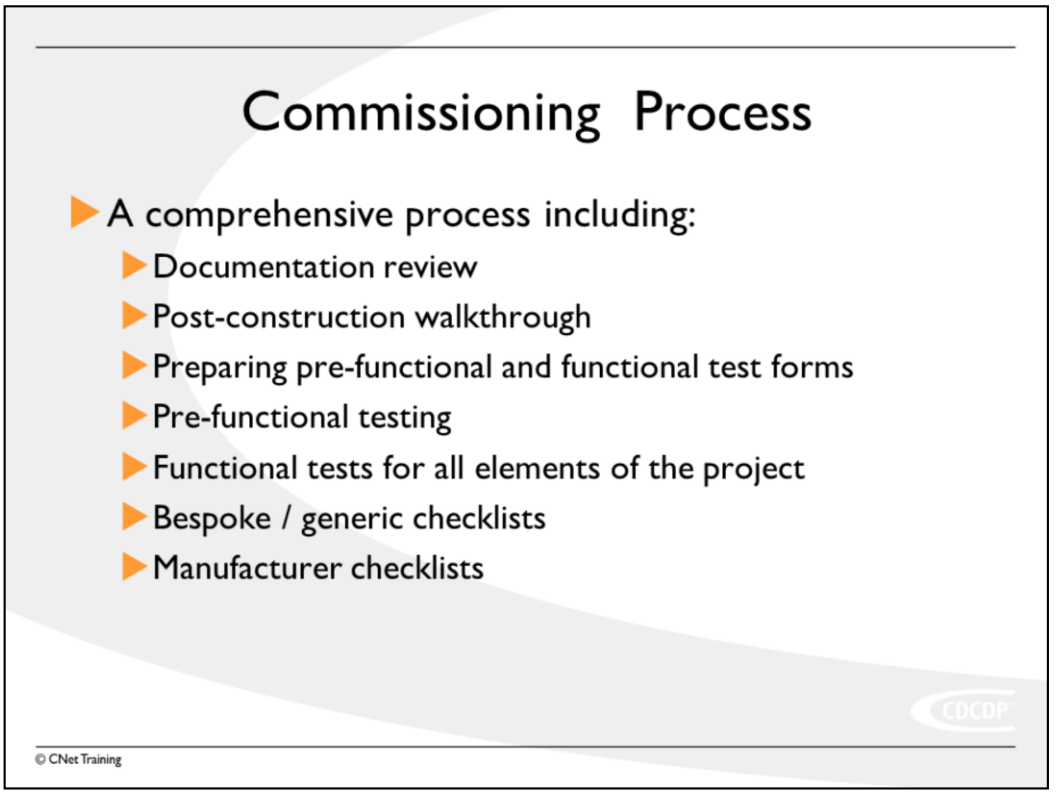
These stakeholders need to work in a coordinated fashion for the commissioning exercise to be successful. The commissioning agent (external verifier) leads the process, while the owner and vendor teams typically perform testing. Documentation is the responsibility of both the commissioning agent and the owner teams. The design and contractor teams are involved much earlier in the process, providing inputs to the commissioning script and scheduling dates.



Establishing a commissioning plan is a critical element to ensuring the Data Centre performs against the agreed design parameters.

In order to hand over the Data Centre to the operator, we must make sure all commissioning is completed correctly, all results and variations are documented, and a complete information pack is prepared.

The CDCD must specify the information required and make sure contractors provide this information in the required format.



Think back to Day One, where the need for a project plan around the design and build was discussed - the handover to the operator is the closing process for this plan.

There can be many commissioning tests required to demonstrate the Data Centre meets the design requirement, providing a basis of operation for the facility to maintain or build upon. The tests can be against Standards, manufacturer recommendations, and bespoke requirements from either the CDCD or the customer. Whichever is used, it is necessary to provide evidence of compliance.

Establish a Test Sequence

- Careful attention needs to be undertaken when planning any commissioning test sequences
  - Need to align with the design scope
  - Awareness of operational impacts
  - Coordinated planning of electrical and mechanical tests
  - Appreciation of the interdependencies between systems
  - Have a recovery plan in place
  - Site walk-rounds with key system owners
  - Establish a test sequence template
- It is essential test sequences are undertaken in a logical and detailed order

© CNet Training

The test sequence needs to be well-planned. This should be supported by a detailed and logical test sequence checklist, with a clear understanding of the required test acceptance outcomes.

Establish a Commissioning Checklist

Line number	Check off box	Description	Results	Proceed?	Initials
132	✓	**Basic operational tests – manual transfers**	n/a	Yes	_____
133	✓	(carry out the following functional tests)	n/a	Yes	_____
134a	✓	ATS racked in "CONNECTED" position	pass	Yes	_____
134b	✓	ATS not bypassed	pass	Yes	_____
134c	✓	Closed-transition transfer capability disabled	pass	Yes	_____
135	✓	**Test steps**	n/a	Yes	_____
136a	✓	Verify that above conditions are satisfied	pass	Yes	_____
137b	✓	Move ATS to "TEST" position	fail	**No**	_____
137c	____	Bypass ATS to Normal source			
137d	____	Move ATS to "TEST" position			
137e	____	Move ATS to "DISCONNECTED" position			

- Detailed with clear acceptance criteria
- Listed in sequence of commissioning activities
- Clear retesting procedure

© CNet Training

Checklists should be utilised to verify each element of the design specification during the commissioning and subsequent handover process. The checklists should detail the precise and agreed test sequence.

Commissioning Process

- A comprehensive process including:
  - Post-construction review
  - Post-occupancy review
  - Pre-warranty review
- Progressive acceptance will occur throughout the project lifecycle, as environments are sequentially brought online during implementation phases
- The commissioning and handover processes may also continue after the Data Centre is occupied

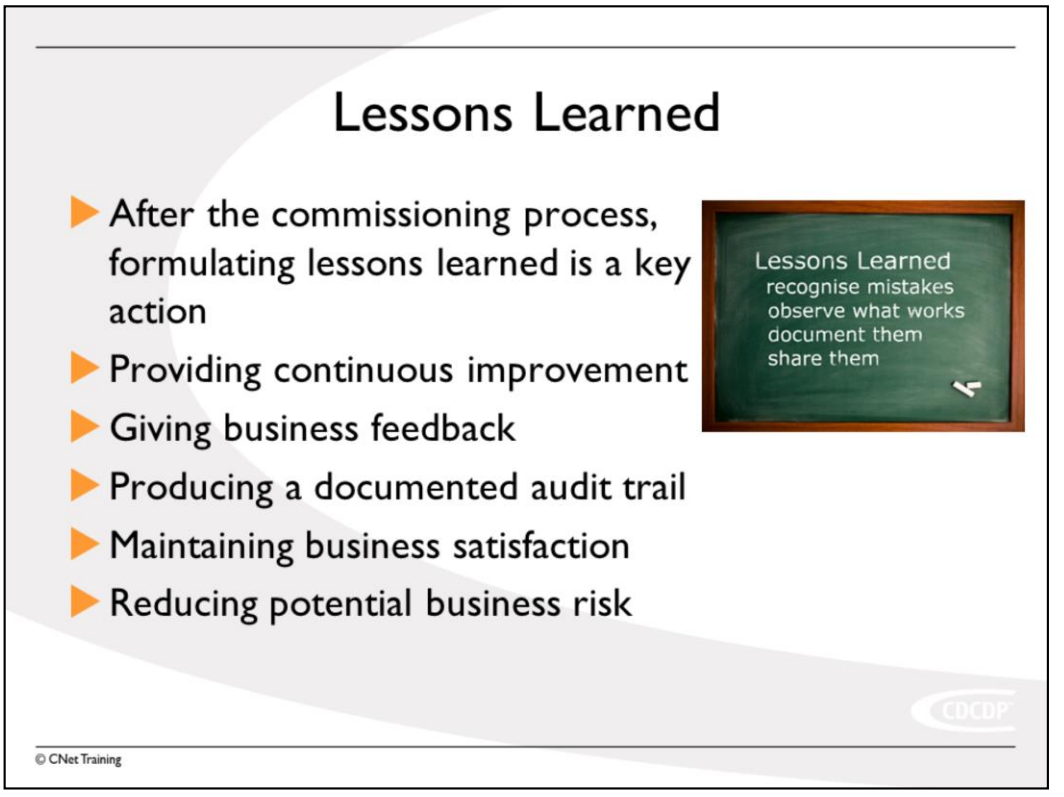
© CNet Training

Commissioning and handover for a Data Centre will be an ongoing process, as some environments need to complete their validation prior to commencement of other design deliverables' implementation phases.

Commissioning Verification

- Verify that processes are completed
  - Develop 'snag list'
  - Conclude project or phase
  - Close procurements
  - Collate documentation
    - As-Built drawings
    - Operational & Maintenance (O&M) certification
    - Test results
    - Vendor and Control records
  - Record lessons learned
  - Prepare formal handover of documentation to the Operator

© CNet Training



There are key benefits to recording lessons learned after the design and commission processes:

- Provides continuous improvement
- Offers the business good feedback and useful information for future audit processes
- Documents design specific issues that may be relevant to the process
- Increases business and customer satisfaction, providing both with useful information as they endeavour to maximise improvement opportunities
- Reduction of future business risk

Commissioning Agent

- Not all operators have the experience level required to witness and verify the commissioning process
- External commissioning agents can provide a neutral view to ensure:
  - The validation of the installation against design
  - Proof of electrical and mechanical functional performance
  - Acceptance of infrastructure and operating systems
  - Endorsement of entire functional performance
  - Verification of test results and documentation

© CNet Training

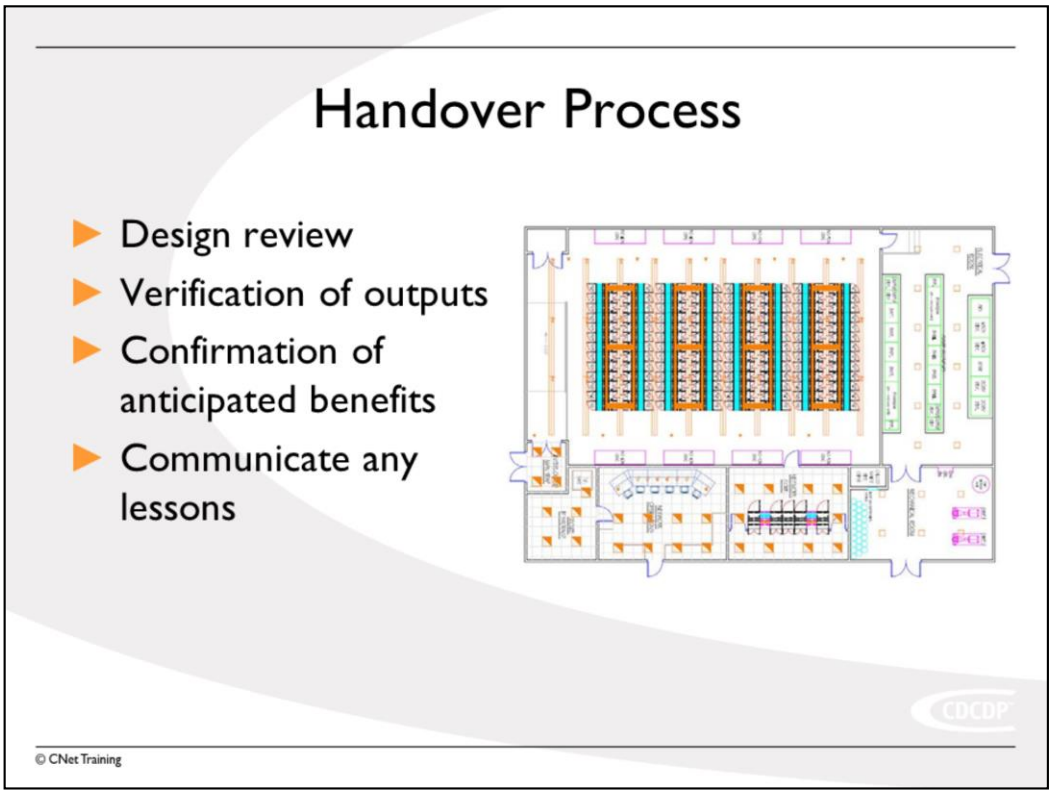
The operator must be made fully aware of all design limits before they take over responsibility.

- Room – Layout, access, zoning
- Architectural and structural - Weight
- Mechanical - Cooling, fire detection/suppression
- Electrical – Power distribution
- Environmental – Temperature, humidity, etc.

Operator Training

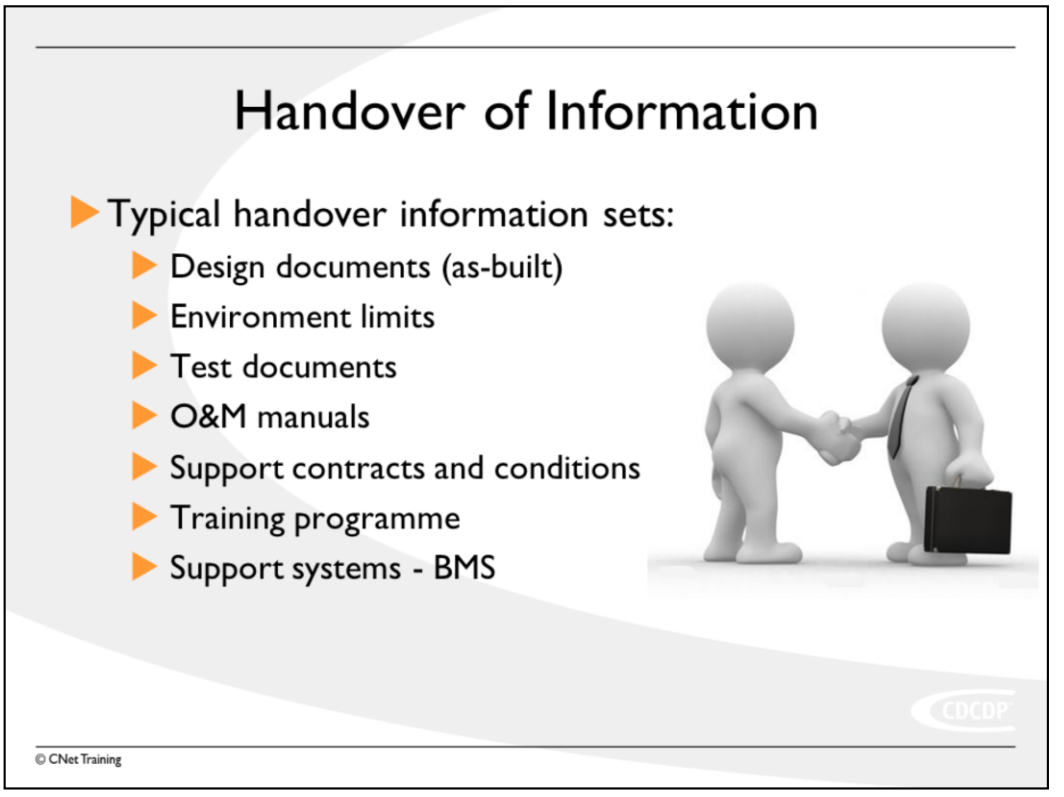
- Once commissioning is completed, it is essential operator training is implemented:
  - Inspection of entire implemented design
  - Full integrated component and load testing
  - Documentation of O&M manuals
  - Compliance assurance of design documents
  - Facility and system training and operational start-up

© CNet Training



On completion of the design project, there are some key aspects that must be formally addressed:

- Review the efficiency of the project in terms of meeting the original time, cost and scope of the design specification.
- Confirm the outputs of the design have been handed over (where appropriate) to ongoing management.
- Confirm the anticipated benefits have been built into the organisation's operational design requirements.
- Record and communicate any lessons beneficial to other future Data Centre projects.



There are many different sources of information, and the CDCD must ensure they are correct at the handover stage.

Review

- Can you?
  - Understand the need for a detailed commissioning process
  - Understand the need for a detailed handover process

© CNet Training

Any Questions?

© CNet Training

Case Study - Exercise 9

© CNet Training

Certified Data Centre Design (CDCD®) Core Unit

Review and Final Assessment

Version 1509

CDCDP

Course Review

- Did we achieve what we set out to do?
- The purpose of this course is to ensure you can:
  - Appreciate the purpose of a Data Centre
  - Operate as part of a multi-disciplinary team
  - Establish a common vocabulary to hold a meaningful discussion with all parties in the team
  - Demonstrate an understanding of key technology areas
  - Use current thinking and relevant Standards to enable a flexible approach to design
  - Demonstrate sufficient knowledge to pass the Certified Data Centre Design (CDCD®) qualification

© CNet Training

Final Assessment

- Scroll to bottom of the Classroom page and open 'Quiz 1 – CDCD'
- Read quiz instructions
- Start Quiz and confirm
- Last question - click 'Next'
- Summary of question responses listed, review
- Submit and finish, then confirm

© CNet Training

Any Questions?

© CNet Training